DOCUMENTO 34 · MAPEO REGULATORIO

Mapeo regulatorio

Cada obligación vinculada a una fase, un rol, una evidencia y una herramienta de SEVEN-G

Fernando García Varela Versión 0.7 (borrador de trabajo) 19-11-2026 Borrador para revisión

7	2-12-2027	13	1
referencias normativas mapeadas	aplicación del alto riesgo del anexo III	etapas y fases en la matriz resumen	procedimiento de mantenimiento del mapeo

EN ESTE DOCUMENTO

01 Objeto y alcance

02 Determinaciones previas a cualquier mapeo

03 Reglamento Europeo de IA

04 ISO/IEC 42001:2023

05 NIST AI RMF 1.0 y perfil de IA generativa NIST AI 600-1

06 RGPD y guías del CEPD

07 DORA y NIS2

08 Normativa española y AESIA

09 Matriz resumen: etapas y fases × referencias

10 Procedimiento de mantenimiento del mapeo

11 Anexo A · Otras jurisdicciones (orientativo)

12 Anexo B · Referencias sectoriales (orientativo)

13 Anexo C · Fuentes consultadas y estado de verificación

14 Herramientas y plantillas asociadas

15 Documentos relacionados

16 Control de versiones

Aviso legal y exención de responsabilidad. SEVEN-G es un marco metodológico de referencia que se ofrece «tal cual» y con fines exclusivamente informativos. No constituye asesoramiento jurídico, regulatorio, financiero ni profesional, ni garantiza el cumplimiento de ninguna norma. Las referencias a regulación general (como el Reglamento Europeo de IA, el RGPD, DORA o NIS2), a normas técnicas y a regulación específica de cada sector o jurisdicción pueden ser incompletas, no aplicar a un caso concreto o quedar desactualizadas por cambios normativos, interpretaciones o criterios de las autoridades posteriores a su fecha de consulta. **Cada organización que use SEVEN-G es la única responsable de identificar la normativa que le aplica, verificar su vigencia y certificar su propio cumplimiento regulatorio**, con el asesoramiento cualificado que corresponda. Esta metodología es una ayuda genérica y gratuita, compartida con la comunidad para que nadie tenga que empezar desde cero; cada persona u organización puede y debe adaptarla a su propio uso. No debe entenderse que sus partes jurídicamente sensibles hayan sido revisadas por una asesoría jurídica: esas revisiones, para cada empresa o sector, son responsabilidad última de la empresa, el consultor o la organización que la use. Aunque se procura mantenerla al día, alguna norma puede haber cambiado sin que se recoja aquí. En la máxima medida permitida por la ley, el autor no asume responsabilidad alguna por los efectos de su aplicación en ninguna organización ni por su aplicabilidad completa. La metodología no otorga certificación de ningún tipo. El autor no asume responsabilidad alguna por el uso que se haga de este contenido ni por las decisiones que se adopten con él. Los datos, cifras, compañías y casos de los ejemplos son ficticios o ilustrativos.

LO ESENCIAL **Condicional: depende de un disparador**

Disparador: la clasificación regulatoria de un sistema no es «riesgo mínimo», se tratan datos personales o la compañía está sujeta a regulación sectorial. Las determinaciones previas (sección 2) se hacen siempre; el resto se consulta por la norma que aplique. No constituye asesoramiento jurídico.

Matriz de obligatoriedad y lectura por capas (documento 94)

01

Objeto y alcance

Alcance y responsabilidad. Este mapeo es **orientativo** y no constituye asesoramiento jurídico. Recoge el estado de las normas consultado el 16 de septiembre de 2026 (fecha de consulta) y no se actualiza automáticamente. Tanto la regulación general (Reglamento Europeo de IA, RGPD, DORA, NIS2 o normativa nacional) como la **regulación específica de cada industria** (banca, seguros, sanidad, energía, sector público, entre otras) cambian: las fechas de aplicación, los artículos y los textos en tramitación se modifican, y su alcance depende de la interpretación, las directrices y los criterios de supervisión de las autoridades competentes. El anexo de referencias sectoriales (sección 12) y el de otras jurisdicciones (sección 11) son solo orientativos y no identifican todas las obligaciones aplicables. Antes de usar cualquier fila en una decisión, verifique su vigencia en la fuente oficial. **La organización usuaria es la única responsable de identificar la normativa que le aplica, realizar la clasificación regulatoria de cada sistema (01 §13) y verificar y certificar su cumplimiento con asesoramiento jurídico cualificado**; el autor no asume esa responsabilidad (documento 93, sección 11).

1.1 Principio: SEVEN-G mapea, no incrusta

SEVEN-G no reproduce la regulación dentro de sus fases. Vincula cada obligación a **una fase o etapa, un rol responsable, una evidencia y una herramienta**. Cuando una norma cambia, se actualiza la fila afectada de este documento y la herramienta T07, sin rehacer el ciclo de vida, los *gates* ni las plantillas.

Este documento desarrolla la sección 13 del documento 01 y cubre: el Reglamento (UE) 2024/1689 (Reglamento Europeo de IA) modificado por el Reglamento (UE) 2026/1744 (sección 3); ISO/IEC 42001:2023 (sección 4); NIST AI RMF 1.0 y NIST AI 600-1 (secciones 5.1 y 5.2); el marco de ciberseguridad NIST CSF 2.0 y su perfil para la IA, el Cyber AI Profile , que a fecha de consulta es un borrador (sección 5.3); los desgloses por subcategoría del AI RMF y del CSF para construir perfiles (secciones 5.4 y 5.5); el RGPD y las guías del CEPD (sección 6); DORA y NIS2 cuando apliquen (sección 7); la normativa española y AESIA (sección 8); y, de forma orientativa, otras jurisdicciones y sectores (secciones 11 y 12).

1.2 Qué no hace este documento

No clasifica sistemas concretos (eso se hace en la fase 3 con P11 y T07), no sustituye el texto de las normas ni las directrices de las autoridades, no afirma requisitos sectoriales no verificados y no reproduce el texto de normas ISO/IEC: solo identifica cláusulas y grupos de controles por número y tema.

1.3 Cómo leer las tablas de mapeo

Todas las tablas de mapeo usan las mismas columnas:

Columna	Contenido
Obligación / requisito	Resumen propio de la obligación, no cita literal.
Artículo o cláusula	Referencia exacta en la norma.
A quién aplica	Operador u organización obligada (por ejemplo, proveedor, responsable del despliegue, responsable del tratamiento, entidad financiera).
Fase o etapa SEVEN-G	Fase del ciclo de vida (0–7), puerta (G0–G5, R6, G7) o etapa del ciclo corporativo (C1–C5).
Rol responsable	Rol de caso de uso u órgano de SEVEN-G (01 §8; documento 30). La asesoría jurídica y el delegado de protección de datos forman parte de la segunda línea.
Evidencia	Plantilla P01–P31 o documento de la biblioteca donde queda la prueba.
Herramienta	Herramienta T01–T22 donde se registra (documento 03).

Nota terminológica. La *Oficina de IA* de SEVEN-G es un órgano interno de la compañía (01 §8.3). Para el órgano de la Comisión Europea previsto en el Reglamento de IA se usa siempre *Oficina Europea de IA* .

1.4 Estado de verificación

Cada afirmación sobre fechas o cambios recientes lleva implícito uno de estos estados, detallado en la sección 13:

Estado	Significado
Verificado (oficial)	Confirmado en una fuente oficial: EUR-Lex, Comisión Europea, Parlamento Europeo, BOE, Congreso de los Diputados, AESIA, ISO, NIST o CEPD.
Pendiente de confirmar	No se ha podido confirmar a fecha de consulta. No debe usarse sin verificación previa.
Borrador	Documento que el emisor ha publicado oficialmente como borrador para comentarios (por ejemplo, el Cyber AI Profile del NIST). Se cita como orientación y puede cambiar; **nunca fundamenta un criterio de *gate*** ni una obligación de SEVEN-G.

Todas las afirmaciones de este documento se apoyan en **fuentes oficiales o primarias** (diarios oficiales, autoridades, organismos emisores de normas y marcos), enlazadas y registradas con su fecha de comprobación; no se usan análisis de terceros como fuente. Lo que no ha podido confirmarse en ellas se marca «Pendiente de confirmar».

02

Determinaciones previas a cualquier mapeo

Antes de aplicar las tablas, cada sistema debe tener resueltas cuatro preguntas. Se registran en la fase 0 de forma provisional (P02, P05) y se confirman en la fase 3 (P11).

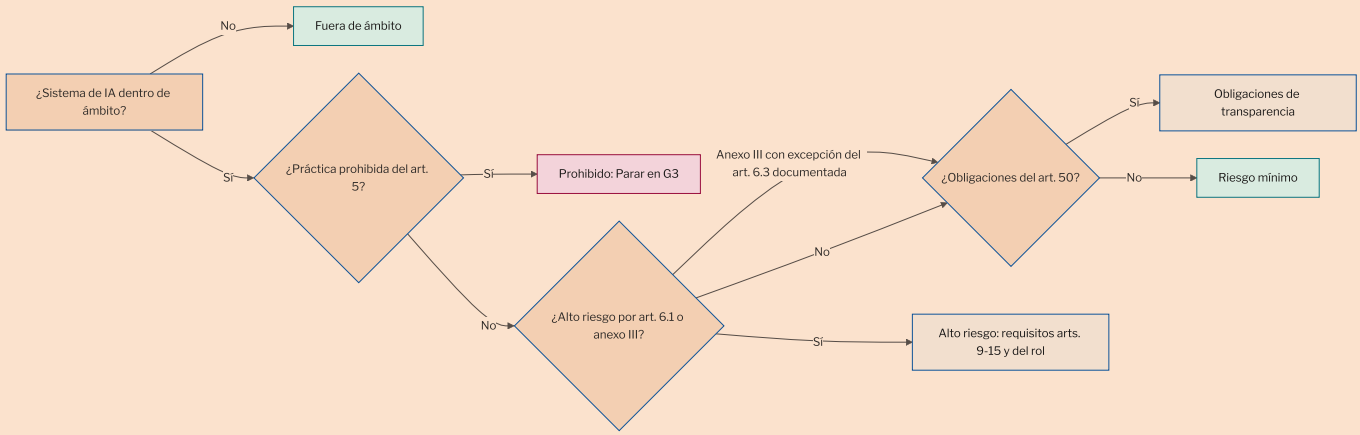
Pregunta	Referencia	Resultado posible	Fase	Evidencia	Herramienta
¿Es un sistema de IA o un modelo de IA de uso general?	Reglamento de IA , art. 3.1 y 3.63; directrices de la Comisión sobre la definición de sistema de IA (febrero de 2025)	Sistema de IA · Modelo de uso general · No es IA (etiqueta *Reglas (no es IA)*)	0, confirmado en 3	P05, P11	T02, T07

Pregunta	Referencia	Resultado posible	Fase	Evidencia	Herramienta
¿Está dentro del ámbito del Reglamento?	Art. 2 (exclusiones: defensa y seguridad nacional, investigación científica, actividad personal no profesional, entre otras)	Dentro · Fuera de ámbito	0, confirmado en 3	P02, P11	T07
¿Qué papel tiene la compañía respecto a ese sistema?	Art. 3.3 a 3.8 (proveedor, responsable del despliegue, representante autorizado, importador, distribuidor, operador) y art. 25	Uno o varios roles por sistema	0, confirmado en 3 y revisado en R6	P02, P11, P14	T02, T07, T09
¿En qué categoría de riesgo está?	Arts. 5, 6, 50 y anexos I y III	Prohibido · Alto riesgo · Obligaciones de transparencia · Riesgo mínimo · Fuera de ámbito · Pendiente de clasificar (taxonomía de 03 §3.3)	3; revisión en R6 y G7	P11	T07, T02

Cambio de rol (art. 25). Una compañía que actúa como responsable del despliegue pasa a tener obligaciones de proveedor si pone su nombre o marca en un sistema de alto riesgo, lo modifica de forma sustancial o cambia su finalidad prevista de modo que pase a ser de alto riesgo. Por eso el rol debe revisarse en G4 (diseño), en G5 (antes de producción) y en cada cambio relevante registrado en P27.

Clasificación regulatoria en la fase 3

Secuencia que sigue el clasificador T07



Fuente: SEVEN-G

Las categorías no son excluyentes: T07 debe registrar todas las que apliquen.

03

Reglamento Europeo de IA

3.1 Calendario de aplicación verificado

El Reglamento (UE) 2024/1689 entró en vigor el 1 de agosto de 2024 y se aplica por etapas. El **Reglamento (UE) 2026/1744 (ómnibus digital sobre IA)**, propuesto por la Comisión el 19 de noviembre de 2025, con acuerdo político de 7 de mayo de 2026, adoptado por el Parlamento Europeo el 16 de junio y por el Consejo el 29 de junio de 2026, firmado el 8 de julio, publicado en el Diario Oficial el 24 de julio y **en vigor desde el 27 de julio de 2026**, ha modificado varias fechas.

Fecha	Qué se aplica	Estado de verificación	Consecuencia en SEVEN-G
1-08-2024	Entrada en vigor del Reglamento.	Verificado (oficial)	—
2-02-2025	Disposiciones generales (definiciones y alfabetización en IA, art. 4) y prácticas prohibidas (art. 5).	Verificado (oficial)	Ningún caso de uso con práctica prohibida supera G3. Formación y política de uso (documentos 31 y 50).
2-08-2025	Obligaciones de proveedores de modelos de IA de uso general (capítulo V); gobernanza; autoridades nacionales; régimen sancionador (salvo multas a proveedores de modelos de uso general).	Verificado (oficial)	Requisitos de información a proveedores de modelos (P14, T09).
2-08-2026	Aplicación general del Reglamento, incluidas las obligaciones de transparencia del art. 50 y las facultades de ejecución de la Comisión sobre modelos de uso general.	Verificado (oficial)	Obligaciones del art. 50 exigibles para sistemas en producción: revisar en R6.
2-12-2026	Nuevas prohibiciones añadidas al art. 5 por el ómnibus (generación de material íntimo no consentido y de material de abuso sexual infantil). Fin del periodo transitorio del marcado legible por máquina del art. 50.2 para sistemas introducidos en el mercado antes del 2-08-2026.	Verificado (oficial): art. 5.1, letras b bis) y b ter), y apartados 1 bis y 1 ter; el plazo del art. 50.2 lo fija el nuevo art. 111.4	Incorporar al cuestionario T07 y a las pruebas de la fase 5 de sistemas generativos.

Fecha	Qué se aplica	Estado de verificación	Consecuencia en SEVEN-G
2-08-2027	Obligación de los Estados miembros de tener operativo al menos un espacio controlado de pruebas nacional (antes 2-08-2026). Plazo para modelos de uso general introducidos antes del 2-08-2025 (art. 111.3).	Verificado (oficial) el espacio de pruebas; art. 111.3 según texto original, sin cambios conocidos	—
2-12-2027	Requisitos y obligaciones de los **sistemas de alto riesgo del art. 6.2 y el anexo III** (antes 2-08-2026).	Verificado (oficial)	Casos de uso con puesta en producción prevista después de esta fecha deben diseñarse ya con los requisitos (G4).
2-08-2028	Requisitos de los **sistemas de alto riesgo del art. 6.1 y el anexo I** (productos regulados; antes 2-08-2027).	Verificado (oficial)	Ídem para productos regulados.

Sistemas ya en el mercado. Por el art. 111, los sistemas de alto riesgo anteriores a la fecha de aplicación solo quedan sujetos si sufren cambios significativos de diseño, con reglas propias para autoridades públicas; tras el ómnibus, el art. 111.2 mantiene que solo quedan sujetos si sufren cambios significativos de diseño, y los destinados a autoridades públicas deben cumplir a más tardar el 2-08-2030 (verificado en EUR-Lex). SEVEN-G no usa esta excepción para rebajar controles (01 §14).

3.2 Cambios del ómnibus digital sobre IA relevantes para SEVEN-G

Cambio	Disposición afectada	Aplicación	Estado	Efecto en SEVEN-G
Aplazamiento del alto riesgo	Art. 113	2-12-2027 (anexo III) y 2-08-2028 (anexo I)	Verificado (oficial)	Actualiza T07 y la columna de fechas de P11. No cambia los *gates*.
Alfabetización en IA: la obligación pasa a ser de apoyo al desarrollo de la alfabetización del personal, sin exigir un nivel concreto; se refuerza el papel de la Comisión y los Estados miembros	Art. 4	Desde la entrada en vigor del ómnibus	Verificado (oficial)	La política y el plan de formación siguen siendo evidencia (documentos 31 y 50). Los responsables del despliegue de alto riesgo mantienen la exigencia de competencia de quien supervisa (art. 26.2).

Cambio	Disposición afectada	Aplicación	Estado	Efecto en SEVEN-G
Nuevas prácticas prohibidas: sistemas que generan o manipulan material íntimo no consentido o material de abuso sexual infantil, incluidos sistemas en los que ese resultado sea razonablemente previsible sin salvaguardas adecuadas	Art. 5	2-12-2026	Verificado (oficial)	Nueva pregunta en T07 y prueba específica en la fase 5 de sistemas generativos (P22).
Periodo transitorio del marcado de contenido sintético	Art. 111.4 (sobre el art. 50.2)	2-12-2026 para sistemas introducidos antes del 2-08-2026	Verificado (oficial)	Plan de adecuación en R6 para sistemas existentes.
Tratamiento de categorías especiales de datos para detectar y corregir sesgos, extendido más allá del alto riesgo con criterio de estricta necesidad	Arts. 4 bis y 10	Desde la entrada en vigor del ómnibus	Verificado (oficial)	Requiere base jurídica RGPD documentada y salvaguardas (P16, evaluación de impacto en protección de datos en P11).
Registro en la base de datos de la UE: se mantiene, con información simplificada, para sistemas del anexo III que el proveedor considera no de alto riesgo	Arts. 6.3 y 49.2; anexo VIII, sección B (modificada)	Con el alto riesgo	Verificado (oficial)	P11 conserva la documentación de la excepción del art. 6.3.
Medidas de apoyo a pymes extendidas a pequeñas empresas de mediana capitalización	Varias disposiciones	Desde la entrada en vigor del ómnibus	Verificado (oficial)	Relevante para la intensidad de la documentación; no rebaja criterios de SEVEN-G.
Supervisión reforzada de la Oficina Europea de IA sobre sistemas basados en modelos de uso general del mismo proveedor y sobre sistemas integrados en plataformas y buscadores de muy gran tamaño	Art. 75	Desde la entrada en vigor del ómnibus	Verificado (oficial) en lo esencial	Identificar la autoridad competente en P11.
Espacios controlados de pruebas: plazo nacional a 2-08-2027 y posible espacio de ámbito UE	Art. 57	2-08-2027	Verificado (oficial)	Opción para casos de uso en fase 3–5 (sección 8).

Cambio	Disposición afectada	Aplicación	Estado	Efecto en SEVEN-G
Máquinas: los sistemas de IA en máquinas pasan a tratarse principalmente mediante el Reglamento (UE) 2023/1230 ; definición de componente de seguridad acotada	Art. 3.14 (sustituido) y anexo I (el Reglamento (UE) 2023/1230 pasa a la sección B)	Según el art. 113 modificado	Verificado (oficial)	Solo relevante para fabricantes de productos.
Plantilla del plan de vigilancia posterior a la comercialización	Art. 72.3 (sustituido)	Orientaciones con plantilla a más tardar el 2-09-2027	Verificado (oficial): el acto de ejecución se sustituye por orientaciones de la Comisión	P25 y P26 no dependen del formato final.

3.3 Directrices, códigos de práctica y plantillas de la Comisión

Documento	Fecha	Estado a 16-09-2026	Uso en SEVEN-G
Directrices sobre prácticas de IA prohibidas	Febrero de 2025	Publicadas (no vinculantes)	T07, P11
Directrices sobre la definición de sistema de IA	Febrero de 2025	Publicadas (no vinculantes)	P05, T02
Código de buenas prácticas para modelos de IA de uso general	Julio de 2025	Publicado (voluntario)	P14: preguntar si el proveedor lo ha suscrito
Directrices sobre el alcance de las obligaciones de los modelos de uso general	Julio de 2025	Publicadas	P14, sección 3.12
Plantilla del resumen público del contenido de entrenamiento de modelos de uso general	Julio de 2025	Publicada	P14
Proyecto de orientaciones y plantilla sobre notificación de incidentes graves (art. 73)	Consulta en 2025	Versión final pendiente de confirmar	P26, T08
Proyecto de directrices sobre clasificación de sistemas de alto riesgo (art. 6)	Proyecto publicado el 19-05-2026; consulta dirigida	Proyecto; adopción final pendiente	T07, P11

Documento	Fecha	Estado a 16-09-2026	Uso en SEVEN-G
Código de buenas prácticas sobre marcado y etiquetado de contenido generado por IA	10-06-2026	Publicado (voluntario)	P18, P22
Directrices sobre las obligaciones de transparencia (art. 50)	20-07-2026	Publicadas	T07, P11, P17
Normas armonizadas (CEN-CENELEC JTC 21)	En elaboración	Pendiente de confirmar publicación en el Diario Oficial	Sección 10: vigilancia normativa

3.4 Prácticas prohibidas (art. 5)

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
No usar técnicas subliminales, manipuladoras o engañosas que alteren de forma sustancial el comportamiento y causen perjuicio considerable	Art. 5.1.a	Todos los operadores	1 (filtrado), 3 (clasificación)	Responsable de producto; Responsable de riesgos con asesoría jurídica	P06, P11	T07
No explotar vulnerabilidades por edad, discapacidad o situación social o económica	Art. 5.1.b	Todos los operadores	1, 3	Responsable de producto; Responsable de riesgos	P06, P11	T07
No realizar puntuación social con trato perjudicial o desproporcionado	Art. 5.1.c	Todos los operadores	1, 3	Responsable de riesgos	P11	T07
No evaluar el riesgo de que una persona cometa un delito basándose únicamente en perfiles o rasgos de personalidad	Art. 5.1.d	Todos los operadores	3	Responsable de riesgos	P11	T07

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
No crear o ampliar bases de datos de reconocimiento facial mediante extracción no selectiva de imágenes	Art. 5.1.e	Todos los operadores	3; controles de datos en 4	Responsable técnico; Responsable de riesgos	P11, P16	T07
No inferir emociones en el lugar de trabajo o en centros educativos, salvo por motivos médicos o de seguridad	Art. 5.1.f	Todos los operadores	3	Responsable de riesgos; segunda línea	P11	T07
No categorizar biométricamente para deducir raza, opiniones políticas, afiliación sindical, convicciones, vida u orientación sexual	Art. 5.1.g	Todos los operadores	3	Responsable de riesgos	P11	T07
No usar identificación biométrica remota en tiempo real en espacios públicos con fines policiales, salvo excepciones tasadas	Art. 5.1.h y 5.2–5.7	Autoridades policiales	3	Responsable de riesgos	P11	T07
No introducir ni usar sistemas que generen material íntimo no consentido o material de abuso sexual infantil, ni sistemas sin salvaguardas razonables frente a ese resultado previsible	Art. 5.1, letras b bis) y b ter), y apartados 1 bis y 1 ter, introducidos por el Reglamento (UE) 2026/1744; aplicación 2-12-2026	Proveedores y responsables del despliegue	3; pruebas en 5; revisión en R6	Responsable técnico; Responsable de riesgos	P11, P18, P22	T07, T10

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
Detectar y detener cualquier práctica prohibida en sistemas en producción o en uso no autorizado	Art. 5; 01 §6.5 y §12	Toda la compañía	6, C4	Responsable de operación; Comité de IA; comisión delegada	P27; no conformidad crítica (documento 37)	T08, T21

Regla SEVEN-G. Una práctica prohibida no pasa de la fase 3 en ningún caso (01 §6.5). Su detección en producción es no conformidad crítica con contención inmediata y escalado E-4 del documento 30.

3.5 Alfabetización en IA (art. 4)

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
Adoptar medidas para apoyar el desarrollo de la alfabetización en IA del personal y de quienes operan o usan sistemas por cuenta de la compañía, según su conocimiento, experiencia y contexto de uso	Art. 4 (redacción del Reglamento (UE) 2026/1744)	Proveedores y responsables del despliegue	C2 (política), C3 (plan), fases 4–6 por caso de uso	Alta dirección; Oficina de IA; responsable de personas	Documento 31 (política), documento 50, P20	T20
Formación específica de quienes usan o supervisan cada sistema	Art. 4; art. 26.2 para alto riesgo	Responsables del despliegue	4 (diseño), 5 (formación de usuarios)	Responsable de producto	P17, P20, P21	T20
Seguimiento de la cobertura de formación y del uso corporativo de IA	Art. 4	Proveedores y responsables del despliegue	C4	Oficina de IA	Panel del consejo (documento 60)	T17, T21

3.6 Clasificación de alto riesgo (art. 6 y anexos I y III)

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
Determinar si el sistema es componente de seguridad de un producto, o el propio producto, cubierto por la legislación del anexo I y sujeto a evaluación de conformidad por terceros	Art. 6.1 y anexo I (secciones A y B)	Proveedores; fabricantes de productos	3	Responsable de riesgos; Responsable técnico	P11	T07
Determinar si el uso previsto figura en el anexo III	Art. 6.2 y anexo III	Proveedores y responsables del despliegue	1 (señal temprana), 3 (clasificación)	Responsable de producto; Responsable de riesgos	P06, P11	T07
Documentar, antes de la introducción en el mercado, la excepción cuando un sistema del anexo III no presenta riesgo significativo (tarea procedimental limitada, mejora de una actividad humana previa, detección de patrones sin sustituir la valoración humana o tarea preparatoria); no cabe si hay elaboración de perfiles	Art. 6.3 y 6.4	Proveedores	3; revisión en G4 y R6	Responsable de riesgos con asesoría jurídica; verificación del Auditor de IA	P11	T07, T03
Registrar la excepción en la base de datos de la UE	Art. 49.2	Proveedores	5 (antes de G5)	Responsable técnico	P11, P23	T02
Revisar la clasificación ante cambios de finalidad, alcance, datos o autonomía	Arts. 6 y 25	Proveedores y responsables del despliegue	R6, G7 y cada cambio	Responsable de riesgos	P11, P27	T07, T08

Áreas del anexo III (señales de alerta en la fase 1): 1 biometría · 2 infraestructuras críticas · 3 educación y formación profesional · 4 empleo, gestión de trabajadores y acceso al autoempleo · 5 acceso a servicios privados esenciales y a servicios y prestaciones públicos esenciales (incluidas la evaluación de solvencia y la puntuación crediticia, salvo detección de fraude, y la evaluación de riesgos y fijación de precios en seguros de vida y salud) · 6 garantía del cumplimiento del Derecho · 7 migración, asilo y control fronterizo · 8 administración de justicia y procesos democráticos. Cualquier caso de uso con una de estas señales debe tratarse como Enterprise desde la fase 0 hasta que P11 concluya lo contrario (01 §9.2).

3.7 Requisitos de los sistemas de alto riesgo (arts. 9 a 15)

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
Sistema de gestión de riesgos continuo durante todo el ciclo de vida, con pruebas frente a métricas y umbrales definidos	Art. 9	Proveedores	3 (evaluación), 4 (controles), 5 (pruebas), 6 (seguimiento)	Responsable de riesgos; Responsable técnico	P12, P13, P22; documento 33	T06
Gobernanza y calidad de los datos de entrenamiento, validación y prueba: pertinencia, representatividad, ausencia de errores en la medida de lo posible, examen de sesgos	Art. 10	Proveedores	3 (disponibilidad), 4 (linaje), 5 (pruebas de sesgo)	Responsable técnico	P10, P16, P22; documento 51	T06
Documentación técnica conforme al anexo IV, preparada antes de la introducción en el mercado y actualizada	Art. 11 y anexo IV	Proveedores	4 y 5; mantenimiento en 6	Responsable técnico	P15, P16, P17, P18, P21; documento 53	T03
Registro automático de eventos (*logs*) que permita la trazabilidad	Art. 12	Proveedores (diseño); responsables del despliegue (conservación, art. 26.6)	4 (diseño), 6 (conservación)	Responsable técnico; Responsable de operación	P15, P18, P25	T10

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
Transparencia e instrucciones de uso para los responsables del despliegue	Art. 13	Proveedores	4, 5	Responsable de producto; Responsable técnico	P17, P21, P24	—
Supervisión humana efectiva: medidas proporcionales a riesgo y autonomía, capacidad de interpretar, no usar, anular o detener el sistema	Art. 14	Proveedores (diseño) y responsables del despliegue (aplicación)	4 (diseño), 5 (prueba), 6 (operación)	Responsable técnico; Responsable de producto	P17, P19, P22, P24	T10
Precisión, solidez y ciberseguridad adecuadas, incluida la resistencia a manipulación de datos, modelos y entradas	Art. 15	Proveedores	4 (diseño), 5 (pruebas), 6 (monitorización)	Responsable técnico; seguridad de la información	P18, P22, P25; documento 35	T10

3.8 Obligaciones de los proveedores y de la cadena de valor (arts. 16 a 25)

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
Garantizar el cumplimiento de los requisitos de los arts. 9–15 e identificarse en el sistema o su documentación	Art. 16.a y 16.b	Proveedores	4, 5	Responsable técnico	P21, P23	T03

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
Sistema de gestión de la calidad documentado (estrategia de cumplimiento, diseño, desarrollo, pruebas, gestión de datos, riesgos, vigilancia posterior a la comercialización, incidentes, responsabilidades)	Art. 17	Proveedores	C2 (marco), 4–6 (aplicación)	Oficina de IA; Responsable técnico	Documentos 01, 20, 21, 53; sección 4 de este documento	T01, T03
Conservar la documentación durante diez años desde la introducción en el mercado	Art. 18	Proveedores	5–7	Responsable técnico; Oficina de IA	P21, P30	T01
Conservar los registros generados automáticamente bajo su control, al menos seis meses	Art. 19	Proveedores	6	Responsable de operación	P24, P25	—
Evaluación de conformidad, declaración UE de conformidad y marcado CE	Arts. 16.f–h, 43, 47 y 48	Proveedores	5 (antes de G5)	Responsable técnico; segunda línea	P21, P23	T03
Registro en la base de datos de la UE	Arts. 16.i y 49	Proveedores	5 (antes de G5)	Responsable técnico	P23	T02
Medidas correctoras, retirada o recuperación e información a distribuidores, responsables del despliegue y autoridades cuando el sistema no sea conforme	Art. 20	Proveedores	6; G7 si procede retirada	Responsable de operación; Comité de IA	P27, P30	T08, T22
Cooperar con las autoridades y facilitar documentación y registros	Art. 21	Proveedores	6, C4	Responsable de riesgos; asesoría jurídica	P27; documento 37	T08

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
Designar representante autorizado cuando el proveedor esté fuera de la UE	Art. 22	Proveedores de terceros países	3 (evaluación del proveedor)	Responsable de riesgos	P14	T09
Verificaciones del importador y del distribuidor antes de comercializar	Arts. 23 y 24	Importadores y distribuidores	3, 5	Responsable de riesgos	P14, P23	T09
Asumir obligaciones de proveedor al poner nombre o marca, modificar sustancialmente o cambiar la finalidad a alto riesgo; acuerdos escritos con proveedores de componentes	Art. 25	Responsables del despliegue, distribuidores, importadores y otros terceros	3, 4 y cada cambio (P27)	Responsable de riesgos; asesoría jurídica	P11, P14; documento 36	T07, T09

3.9 Obligaciones de los responsables del despliegue (art. 26)

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
Usar el sistema conforme a las instrucciones de uso con medidas técnicas y organizativas adecuadas	Art. 26.1	Responsables del despliegue de alto riesgo	4, 6	Responsable de operación	P17, P24	—
Encomendar la supervisión humana a personas con competencia, formación, autoridad y apoyo	Art. 26.2	Responsables del despliegue de alto riesgo	4 (diseño), 5 (formación), 6	Responsable de producto	P03, P17, P20	T20

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
Garantizar que los datos de entrada bajo su control sean pertinentes y suficientemente representativos	Art. 26.4	Responsables del despliegue de alto riesgo	4, 6	Responsable técnico	P16, P25	—
Vigilar el funcionamiento, informar al proveedor, suspender el uso ante riesgo e informar de incidentes graves	Art. 26.5	Responsables del despliegue de alto riesgo	6	Responsable de operación	P25, P26, P27	T08
Conservar los registros bajo su control al menos seis meses, salvo otra norma	Art. 26.6	Responsables del despliegue de alto riesgo	6	Responsable de operación	P24, P25	—
Informar a los representantes de los trabajadores y a los trabajadores afectados antes de usar un sistema de alto riesgo en el lugar de trabajo	Art. 26.7	Empleadores que despliegan alto riesgo	4 (plan), antes de G5	Patrocinador; responsable de personas	P20, P23; documento 50	T20
Registro en la base de datos de la UE cuando el responsable del despliegue es una autoridad pública	Art. 26.8 y art. 49.3	Autoridades y organismos públicos	5	Responsable técnico	P23	T02
Usar la información del proveedor para la evaluación de impacto en protección de datos	Art. 26.9; RGPD art. 35	Responsables del despliegue	3	Responsable de riesgos; delegado de protección de datos	P11	T07

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
Informar a las personas físicas de que están sujetas al uso de un sistema del anexo III que toma decisiones o ayuda a tomarlas	Art. 26.11	Responsables del despliegue de alto riesgo	4 (diseño), 6	Responsable de producto	P17, P24	—
Explicación de decisiones individuales a la persona afectada, cuando proceda	Art. 86	Responsables del despliegue de alto riesgo del anexo III	4 (diseño), 6 (atención de solicitudes)	Responsable de producto; segunda línea	P17, P24	T08
Cooperar con las autoridades	Art. 26.12	Responsables del despliegue	6, C4	Responsable de riesgos	P27	T08

Entidades financieras. Algunas obligaciones se consideran cumplidas con el gobierno interno exigido por la legislación financiera (por ejemplo, arts. 17.4 y 26.5); P11 debe identificar qué evidencia sectorial cubre cada una.

3.10 Evaluación de impacto en derechos fundamentales (art. 27)

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
Realizar la evaluación antes del primer uso: procesos, periodo y frecuencia de uso, personas y colectivos afectados, riesgos específicos, medidas de supervisión humana y medidas ante materialización de riesgos	Art. 27.1	Organismos de Derecho público, entidades privadas que prestan servicios públicos y responsables del despliegue de sistemas del anexo III, punto 5, letras b) y c); no aplica al área 2 del anexo III	3 (evaluación), actualizada en 4	Responsable de riesgos; segunda línea; Responsable de producto	P11, P48	T07

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
Actualizar la evaluación cuando cambien sus elementos	Art. 27.2	Mismos	R6 y cada cambio	Responsable de riesgos	P11, P48, P27	T07, T08
Notificar los resultados a la autoridad de vigilancia del mercado con el formulario previsto	Art. 27.3	Mismos	5 (antes de G5)	Responsable de riesgos	P11, P48, P23	T07
Complementar, sin duplicar, la evaluación de impacto en protección de datos, a la que el art. 27.4 modificado permite remitirse	Art. 27.4; RGPD art. 35	Mismos	3	Responsable de riesgos; delegado de protección de datos	P11, P48, P47	T07

Se aplica con el alto riesgo (2-12-2027 para el anexo III); la plantilla de la Oficina Europea de IA está **pendiente de confirmar**. Todo caso de uso Enterprise con decisiones sobre personas debería aplicar este contenido en P11 y P48 aunque no esté obligada.

3.11 Transparencia (art. 50)

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
Informar a las personas de que interactúan con un sistema de IA, salvo que sea evidente	Art. 50.1	Proveedores de sistemas que interactúan con personas	4 (diseño), 5 (prueba)	Responsable de producto	P17, P22, P49	T07

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
Marcar en formato legible por máquina los contenidos sintéticos de audio, imagen, vídeo o texto	Art. 50.2; periodo transitorio hasta 2-12-2026 para sistemas anteriores al 2-08-2026 (art. 111.4)	Proveedores de sistemas generativos	4, 5; plan de adecuación en R6	Responsable técnico	P18, P22	T07, T10
Informar a las personas expuestas a sistemas de reconocimiento de emociones o de categorización biométrica	Art. 50.3	Responsables del despliegue	4, 6	Responsable de producto; delegado de protección de datos	P17, P24, P49	T07
Revelar que un contenido es ultrasuplantación (*deepfake*), y que un texto publicado para informar sobre asuntos de interés público ha sido generado o manipulado, salvo revisión humana con responsabilidad editorial	Art. 50.4	Responsables del despliegue	4, 6	Responsable de producto	P17, P24, P49	T07
Facilitar la información de forma clara y a más tardar en la primera interacción o exposición	Art. 50.5	Proveedores y responsables del despliegue	5 (prueba)	Responsable de producto	P22	—

Referencias de apoyo: directrices de la Comisión sobre el art. 50 (20-07-2026) y código de buenas prácticas sobre marcado y etiquetado (sección 3.3). El art. 50 obliga a informar a las personas que interactúan con un sistema de IA; **no obliga a un agente de IA a identificarse ante un servicio**. Que la

ley exija a los agentes identificarse ante los servicios es una propuesta del sector, no una obligación vigente (35 §9.4).

3.12 Modelos de IA de uso general (arts. 51 a 55) para quien los integra

La mayoría de las compañías son **proveedoras posteriores** o responsables del despliegue de sistemas construidos sobre modelos de terceros: les afecta la información que deben recibir y el riesgo de convertirse en proveedoras.

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
Obtener del proveedor del modelo la información y documentación para proveedores posteriores (capacidades, limitaciones, integración)	Art. 53.1.b y anexo XII	Obligación del proveedor del modelo; la compañía integradora debe exigirla	3 (evaluación del proveedor), 4 (arquitectura)	Responsable técnico; Responsable de riesgos	P14, P15, P16	T09
Comprobar que el proveedor tiene política de derechos de autor y resumen público del contenido de entrenamiento	Art. 53.1.c y 53.1.d	Obligación del proveedor del modelo	3	Responsable de riesgos; asesoría jurídica	P14; documento 36	T09
Conocer si el modelo está clasificado con riesgo sistémico y qué evaluaciones, mitigaciones y notificación de incidentes aplica su proveedor	Arts. 51, 52 y 55	Obligación del proveedor del modelo	3, 6	Responsable de riesgos	P12, P14	T06, T09

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
Evaluar si las modificaciones propias (por ejemplo, reentrenamiento o ajuste fino significativo) convierten a la compañía en proveedora del modelo modificado, con los criterios de las directrices de la Comisión de julio de 2025	Arts. 3.63, 3.66, 3.68 y 53; directrices sobre modelos de uso general	Compañías que modifican modelos	4 (diseño), cada cambio	Responsable técnico con asesoría jurídica	P11, P15, P16	T07
Si el sistema construido sobre el modelo es de alto riesgo, cumplir todas las obligaciones del proveedor del sistema	Arts. 6, 16 y 25	Proveedores posteriores	3–6	Responsable técnico; Responsable de riesgos	Secciones 3.7 y 3.8	T07
Considerar la adhesión del proveedor al código de buenas prácticas como elemento de la evaluación, no como garantía	Art. 56; código de julio de 2025	Compañías integradoras	3	Responsable de riesgos	P14	T09

Calendario: obligaciones de proveedores de modelos desde el 2-08-2025; facultades de ejecución de la Comisión desde el 2-08-2026; modelos introducidos antes del 2-08-2025, hasta el 2-08-2027.

3.13 Registro en la base de datos de la UE (arts. 49 y 71)

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
Registrar el proveedor y el sistema de alto riesgo del anexo III (salvo área 2, que se registra a nivel nacional) antes de introducirlo en el mercado o ponerlo en servicio	Art. 49.1, art. 71 y anexo VIII	Proveedores	5, antes de G5	Responsable técnico	P23	T02, T03
Registrar los sistemas del anexo III que el proveedor considera no de alto riesgo por el art. 6.3, con la información simplificada que establezca el texto modificado	Art. 49.2 y anexo VIII, sección B (modificada por el Reglamento (UE) 2026/1744)	Proveedores	5, antes de G5	Responsable técnico	P11, P23	T02
Registrarse y seleccionar el sistema en la base de datos cuando el responsable del despliegue es autoridad pública	Art. 49.3	Autoridades y organismos públicos	5, antes de G5	Responsable técnico	P23	T02
Mantener actualizada la información registrada	Arts. 49 y 71	Proveedores y autoridades públicas	6, R6, G7	Responsable de operación	P27, P30	T02, T08

El alta en el inventario interno (P05, T02) es obligatoria desde la fase 0 para todo sistema; el registro UE es distinto y se verifica en G5.

3.14 Vigilancia posterior a la comercialización (art. 72)

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
Establecer y documentar un sistema de vigilancia posterior a la comercialización proporcionado, que recoja y analice datos de funcionamiento durante toda la vida útil	Art. 72.1 y 72.2	Proveedores de alto riesgo	4 (diseño), 6 (ejecución)	Responsable de operación; Responsable técnico	P24, P25, P28	T12
Plan de vigilancia posterior a la comercialización como parte de la documentación técnica	Art. 72.3 y anexo IV	Proveedores de alto riesgo	4, verificado en G5	Responsable técnico	P21, P25	T03
Integrar la vigilancia en los sistemas existentes cuando exista legislación sectorial equivalente	Art. 72.4	Proveedores sujetos al anexo I, sección A, y entidades financieras	4	Responsable de riesgos	P11, P25	—
Revisar periódicamente los resultados de la vigilancia y la vigencia de la clasificación	Art. 72; 01 §6.8	Proveedores	R6	Auditor de IA verifica; Comité de IA decide en Enterprise	P29	T03

3.15 Incidentes graves (art. 73)

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
Clasificar si un incidente es "incidente grave" (fallecimiento o daño grave a la salud; alteración grave e irreversible de infraestructuras críticas; incumplimiento de obligaciones de Derecho de la Unión que protegen derechos fundamentales; daño grave a la propiedad o al medio ambiente)	Art. 3.49	Proveedores y responsables del despliegue	6	Responsable de operación; Responsable de riesgos; asesoría jurídica	P26, P27	T08
Notificar a la autoridad de vigilancia del mercado en cuanto se establezca el vínculo causal o su probabilidad razonable y, como máximo, en 15 días desde que se tenga conocimiento	Art. 73.1 y 73.2	Proveedores de alto riesgo	6 (severidad S1)	Responsable de riesgos; asesoría jurídica	P26, P27	T08
Plazos reducidos: inmediato y no más de 2 días en infracciones generalizadas o alteraciones graves de infraestructuras críticas; no más de 10 días en caso de fallecimiento	Art. 73.3 y 73.4	Proveedores de alto riesgo	6 (S1)	Responsable de riesgos	P26, P27	T08

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
Investigar, evaluar el riesgo y adoptar medidas correctoras sin alterar el sistema de forma que afecte a la evaluación de las causas antes de informar a las autoridades	Art. 73.6	Proveedores de alto riesgo	6; G7 si procede	Responsable de operación; Responsable técnico	P27; documento 37	T08
Informar sin demora al proveedor y, en su caso, a las autoridades cuando el responsable del despliegue identifique un incidente grave	Art. 26.5	Responsables del despliegue	6	Responsable de operación	P26, P27	T08
Tratar todo posible incidente grave como severidad S1 y escalado E-4	Documentos 30 y 37	Toda la compañía	6, C4	Comité de IA; comisión delegada	P27	T08

Las orientaciones y la plantilla de la Comisión sobre incidentes graves se publicaron en borrador en 2025; su versión final está **pendiente de confirmar**. La obligación de notificación se aplica con las obligaciones de alto riesgo.

3.16 Sanciones (art. 99), a título informativo

Infracción	Artículo	Importe máximo	Uso en SEVEN-G
Prácticas prohibidas	Art. 99.3	35 millones de euros o el 7 % del volumen de negocios mundial anual, si es superior	Impacto 5 (Crítico) en el eje regulatorio (documento 33)
Otras obligaciones de operadores (entre ellas arts. 16, 22–24, 26 y 50)	Art. 99.4	15 millones de euros o el 3 %	Impacto 4 o 5 según el caso
Información incorrecta, incompleta o engañosa a autoridades	Art. 99.5	7,5 millones de euros o el 1 %	Impacto 3 o 4

Infracción	Artículo	Importe máximo	Uso en SEVEN-G
Pymes y empresas emergentes	Art. 99.6	El menor de los dos importes	La extensión a pequeñas empresas de mediana capitalización está **pendiente de confirmar**
Proveedores de modelos de uso general (multas de la Comisión)	Art. 101	15 millones de euros o el 3 %	Riesgo del proveedor en P14

El régimen sancionador español está en tramitación (sección 8). Las sanciones solo se citan para valorar el impacto regulatorio.

04

ISO/IEC 42001:2023

ISO/IEC 42001:2023 (publicada en diciembre de 2023; a fecha de consulta, 25-09-2026, ISO la mantiene publicada, en la etapa 60.60, sin revisión en curso) especifica los requisitos de un sistema de gestión de IA. En SEVEN-G, **el ciclo corporativo C1–C5 actúa como sistema de gestión** y el ciclo de vida 0–7 como proceso operativo (01 §13). La certificación no forma parte de SEVEN-G, pero una compañía que aplica el marco debería poder aportar las evidencias de esta sección.

4.1 Cláusulas 4 a 10

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
Comprender la organización y su contexto, incluido su papel respecto a los sistemas de IA	4.1	Organización que implanta el sistema de gestión	C1	Oficina de IA	Documento 11 (diagnóstico); inventario	T02, T15
Necesidades y expectativas de las partes interesadas	4.2	Ídem	C1, C2	Oficina de IA; alta dirección	Documento 13	T19
Alcance del sistema de gestión	4.3	Ídem	C2	Alta dirección	Documentos 13 y 31	T19
Establecer el sistema de gestión	4.4	Ídem	C2–C5	Comité de IA	Documento 01	T01

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
Liderazgo y compromiso de la dirección	5.1	Alta dirección	C2, C4	Consejo; alta dirección	Documentos 13 y 60	T17, T18
Política de IA	5.2	Alta dirección	C2	Alta dirección; aprueba el consejo	Documento 31	T19
Roles, responsabilidades y autoridades	5.3	Alta dirección	C2; fase 0	Comité de IA	Documento 30; P03	T01
Acciones para abordar riesgos y oportunidades	6.1.1	Organización	C2, C3	Comité de IA	Documentos 13 y 14	T06
Evaluación de riesgos de IA	6.1.2	Organización	C2 (criterios), fase 3 (evaluación)	Responsable de riesgos	Documento 33; P12	T06
Tratamiento de riesgos de IA y declaración de aplicabilidad de los controles	6.1.3	Organización	C2 (declaración), fases 3–4	Oficina de IA; Responsable de riesgos	P13; P74 (declaración de aplicabilidad), con la sección 4.2 como base	T06
Evaluación de impacto de los sistemas de IA	6.1.4	Organización	Fase 3	Responsable de riesgos	P11	T07
Objetivos de IA y planificación para lograrlos	6.2	Organización	C2, C3; fase 2	Alta dirección; Responsable de producto	Documentos 13 y 14; P08	T11, T19
Planificación de los cambios	6.3	Organización	C3, C5	Comité de IA	Documento 14; P27	T01
Recursos	7.1	Organización	C3	Comité de IA	Documento 14	T13
Competencia	7.2	Organización	C3; fases 4–5	Responsable de personas; Oficina de IA	Documento 50; P20	T20
Toma de conciencia	7.3	Organización	C2–C4	Oficina de IA	Documentos 31 y 50	T20, T21
Comunicación	7.4	Organización	C4	Oficina de IA	Documento 60	T17

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
Información documentada	7.5	Organización	Todas	Oficina de IA	Registro de evidencias (03 §4)	T01, T03
Planificación y control operacional	8.1	Organización	Fases 0–7	Responsables del caso de uso	Documento 20; P29	T01, T03
Evaluación de riesgos de IA a intervalos planificados	8.2	Organización	Fase 3; R6	Responsable de riesgos	P12	T06
Tratamiento de riesgos de IA	8.3	Organización	Fases 3–6	Responsable de riesgos	P13	T06
Evaluación de impacto de los sistemas de IA a intervalos planificados	8.4	Organización	Fase 3; R6	Responsable de riesgos	P11	T07
Seguimiento, medición, análisis y evaluación	9.1	Organización	C4; fase 6	Oficina de IA	Documentos 40 y 41; P25, P28	T12, T17
Auditoría interna	9.2	Organización	C4, C5	Tercera línea; Auditor de IA	Documento 38	T03
Revisión por la dirección	9.3	Alta dirección	C5	Consejo; alta dirección	Documento 60; documento 11	T15, T17
Mejora continua	10.1	Organización	C5	Oficina de IA	Lecciones aprendidas (P30)	T01
No conformidad y acción correctiva	10.2	Organización	Todas	Auditor de IA; Comité de IA	Documento 37	T08

4.2 Anexo A: controles por grupo

El anexo A agrupa los controles de referencia en nueve grupos. La tabla indica el objetivo de cada grupo en términos propios y dónde lo cubre SEVEN-G. La declaración de aplicabilidad de la compañía se prepara con la plantilla P74, control a control, y debe cotejarse con el texto adquirido de la norma.

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
Políticas relacionadas con la IA: política documentada, alineada con otras políticas y revisada	A.2	Organización	C2, C5	Alta dirección; Oficina de IA	Documento 31	T19
Organización interna: roles y responsabilidades; cauce para comunicar preocupaciones	A.3	Organización	C2; fase 0	Comité de IA	Documento 30; P03; canal de comunicación del documento 31	T01
Recursos para los sistemas de IA: documentación de recursos de datos, herramientas, cómputo y personas	A.4	Organización	Fases 3–4	Responsable técnico	P10, P15, P16	T13
Evaluación de impactos: proceso, documentación, impacto en personas o colectivos e impacto social	A.5	Organización	Fase 3; R6	Responsable de riesgos	P11	T07
Ciclo de vida del sistema de IA: objetivos y procesos de desarrollo responsable, requisitos, diseño, verificación y validación, despliegue, operación y seguimiento, documentación técnica, registro de eventos	A.6	Organización	Fases 2–6	Responsable técnico; Responsable de operación	P08, P15, P17, P18, P21, P22, P24, P25; documento 53	T03, T10
Datos para los sistemas de IA: datos de desarrollo, adquisición, calidad, procedencia y preparación	A.7	Organización	Fases 3–5	Responsable técnico	P16; documento 51	T06
Información para las partes interesadas: documentación para usuarios, comunicación externa, comunicación de incidentes	A.8	Organización	Fases 4–6	Responsable de producto; Responsable de operación	P17, P24, P26	T08

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
Uso de los sistemas de IA: procesos y objetivos de uso responsable, uso previsto	A.9	Organización	C2; fases 4–6	Responsable de producto; Oficina de IA	Documento 31; P17	T21
Relaciones con terceros y clientes: reparto de responsabilidades, proveedores y clientes	A.10	Organización	Fases 3–4; C4	Responsable de riesgos	P14; documento 36	T09

4.3 Normas relacionadas

ISO/IEC 42005:2025 (evaluación de impacto de sistemas de IA) es referencia metodológica de P11; ISO/IEC 23894:2023 (gestión del riesgo en IA), del documento 33; e ISO/IEC 42006:2025 (organismos de auditoría y certificación), del documento 38.

Correspondencia con el NIST AI RMF . El centro de recursos del AI RMF de NIST (AIRC) aloja una correspondencia AI RMF ↔ ISO/IEC 42001 del AIRC aportada por un tercero (Microsoft) y preparada en 2023 sobre el borrador final (FDIS) de la norma, antes de su publicación. NIST advierte que alojarla no implica respaldo. Sirve como orientación para relacionar las subcategorías del AI RMF con las cláusulas y los controles del anexo A, pero debe cotejarse con la norma publicada. El AI RMF no es certificable: lo certificable es el sistema de gestión conforme a ISO/IEC 42001, por una entidad de certificación acreditada (documento 38 §12). SEVEN-G no certifica.

05

NIST AI RMF 1.0 y perfil de IA generativa NIST AI 600-1

El NIST AI RMF 1.0 (enero de 2023) es un marco voluntario. A fecha de consulta, NIST indica que está en revisión; el perfil NIST AI 600-1 se publicó el 26 de julio de 2024. SEVEN-G los usa como referencia de buenas prácticas, no como obligación. La sección 5.3 añade el marco de ciberseguridad del NIST (CSF 2.0) y su perfil para la IA.

5.1 Funciones y categorías del AI RMF

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
Políticas, procesos y procedimientos de gestión del riesgo de IA	GOVERN 1	Organizaciones que diseñan, desarrollan, despliegan o usan IA (voluntario)	C2	Alta dirección; Oficina de IA	Documentos 01, 31 y 33	T19
Estructuras de rendición de cuentas	GOVERN 2	Ídem	C2; fase 0	Comité de IA	Documento 30; P03	T01
Diversidad e inclusión de los equipos en la gestión del riesgo	GOVERN 3	Ídem	C3; fase 0	Responsable de personas	Documento 50; P03	—
Cultura de gestión y comunicación del riesgo	GOVERN 4	Ídem	C2, C4	Oficina de IA	Documentos 31 y 60	T17
Relación con actores externos y partes afectadas	GOVERN 5	Ídem	Fases 1, 3 y 6	Responsable de producto	P11, P17	—
Riesgos de terceros y cadena de suministro	GOVERN 6	Ídem	Fase 3; C4	Responsable de riesgos	P14; documento 36	T09
Establecer y comprender el contexto	MAP 1	Ídem	Fases 0–1	Responsable de producto	P01, P02, P06	T01
Categorizar el sistema de IA	MAP 2	Ídem	Fases 1 y 3	Responsable de riesgos	P07, P11	T05, T07
Capacidades, uso previsto, objetivos, beneficios y costes	MAP 3	Ídem	Fases 2–3	Responsable de producto	P08, P10	T11, T13
Riesgos y beneficios de todos los componentes, incluidos los de terceros	MAP 4	Ídem	Fase 3	Responsable de riesgos	P12, P14	T06, T09

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
Impactos en personas, colectivos, organizaciones y sociedad	MAP 5	Ídem	Fase 3	Responsable de riesgos	P11	T07
Métodos y métricas adecuados	MEASURE 1	Ídem	Fases 2 y 5	Responsable técnico	P09, P22	T11
Evaluación de las características de fiabilidad (validez, seguridad, resiliencia, transparencia, explicabilidad, privacidad, equidad)	MEASURE 2	Ídem	Fase 5	Responsable técnico	P22	T10
Seguimiento de riesgos a lo largo del tiempo	MEASURE 3	Ídem	Fase 6	Responsable de operación	P25, P27	T06, T08
Retroalimentación sobre la eficacia de la medición	MEASURE 4	Ídem	R6, C5	Oficina de IA	P28; documento 41	T12
Priorizar y responder a los riesgos	MANAGE 1	Ídem	Fases 3 y 6	Responsable de riesgos	P12, P13	T06
Estrategias para maximizar beneficios y minimizar impactos negativos	MANAGE 2	Ídem	Fases 4–7	Responsable de producto; Comité de IA	P13, P19, P30	T22
Gestionar los riesgos de terceros	MANAGE 3	Ídem	Fases 3–6	Responsable de riesgos	P14	T09
Tratamientos documentados y supervisados, incluidas respuesta, recuperación y comunicación	MANAGE 4	Ídem	Fase 6	Responsable de operación	P24, P26, P27	T08

5.2 Perfil de IA generativa (NIST AI 600-1)

El perfil describe riesgos específicos o agravados por la IA generativa y acciones sugeridas asociadas a las categorías del AI RMF. SEVEN-G los incorpora como riesgos tipo de la categoría **GEN** (y **SEG**, **TER**

cuando corresponda) del documento 33.

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
Información o capacidades químicas, biológicas, radiológicas o nucleares	NIST AI 600-1, riesgo "CBRN"	Voluntario	Fase 3 (solo si aplica al uso)	Responsable de riesgos	P12	T06
Confabulación (contenidos erróneos presentados con seguridad)	Riesgo "Confabulation"	Voluntario	Fases 3, 5 y 6	Responsable técnico	P12, P22, P25	T06
Contenido peligroso, violento o de odio	Riesgo "Dangerous, violent or hateful content"	Voluntario	Fases 4–5	Responsable técnico	P18, P22	T10
Privacidad de datos	Riesgo "Data privacy"	Voluntario	Fases 3–4	Responsable de riesgos; delegado de protección de datos	P11, P16	T07
Impactos ambientales	Riesgo "Environmental impacts"	Voluntario	Fase 3; C4	Responsable técnico	P10; documento 42	T13
Sesgo perjudicial y homogeneización	Riesgo "Harmful bias and homogenization"	Voluntario	Fases 3 y 5	Responsable técnico	P12, P22	T06
Configuración persona–IA (dependencia excesiva, antropomorfización)	Riesgo "Human-AI configuration"	Voluntario	Fase 4	Responsable de producto	P17, P20	T20
Integridad de la información	Riesgo "Information integrity"	Voluntario	Fases 4–5	Responsable de producto	P17, P22	—
Seguridad de la información (incluida inyección de instrucciones)	Riesgo "Information security"	Voluntario	Fases 4–6	Responsable técnico; seguridad de la información	P18, P22; documento 35	T10

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
Propiedad intelectual	Riesgo "Intellectual property"	Voluntario	Fases 3–5	Responsable de riesgos; asesoría jurídica	P14; documento 53	T09
Contenido obsceno, degradante o abusivo	Riesgo "Obscene, degrading and/or abusive content"	Voluntario	Fases 3–5 (relacionado con las nuevas prohibiciones del art. 5)	Responsable técnico	P11, P22	T07, T10
Cadena de valor e integración de componentes	Riesgo "Value chain and component integration"	Voluntario	Fases 3–4	Responsable de riesgos	P14, P16	T09

5.3 NIST CSF 2.0 y Cyber AI Profile

El **NIST CSF 2.0** (NIST CSWP 29, publicado en su versión final el 26 de febrero de 2024) es un marco **voluntario** de gestión del riesgo de ciberseguridad. Su núcleo es una taxonomía de resultados que se organiza en seis funciones —**GV** gobernar, **ID** identificar, **PR** proteger, **DE** detectar, **RS** responder y **RC** recuperar—, 22 categorías y 106 subcategorías. Cada organización describe con **perfiles** los resultados que alcanza hoy (**perfil actual**) y los que quiere alcanzar (**perfil objetivo**); la diferencia es la brecha que se convierte en un plan de acción priorizado.

El **Cyber AI Profile** (NIST IR 8596) es el perfil comunitario del CSF 2.0 para la IA. A fecha de consulta (25-09-2026) solo existe su **borrador preliminar inicial**, publicado el 16 de diciembre de 2025, con comentarios cerrados el 30 de enero de 2026; la página del proyecto del NIST indica que se están revisando los comentarios. Organiza las subcategorías del CSF en tres áreas: **Secure**, proteger los componentes de los sistemas de IA; **Defend**, usar la IA en la ciberdefensa de la organización; y **Thwart**, frustrar los ataques que usan IA. Para cada subcategoría y área propone una prioridad (alta, moderada o fundamental). Estado: **Borrador** (sección 1.4). Mientras lo sea, SEVEN-G lo usa como orientación y **no fundamenta en él ningún criterio de *gate*** ni ninguna obligación.

Advertencia sobre los *tiers*. Los *tiers* del CSF (1 Parcial, 2 Informado sobre el riesgo, 3 Repetible, 4 Adaptativo) caracterizan el rigor de las prácticas de gobierno y de gestión del riesgo de ciberseguridad **de toda la organización** o de una unidad. **No son un nivel de madurez de cada subcategoría**, y el NIST AI RMF no tiene *tiers* ni escala de madurez. Puntuar cada subcategoría de 1 a 4 sería una convención propia que no debe presentarse como «*tier* del CSF». SEVEN-G no crea una segunda escala: el grado de cada resultado se expresa con la escala de madurez 0–5 del documento 11.

Por qué importa. Muchas compañías ya gestionan su ciberseguridad con el CSF y su comité de riesgos lee los resultados en sus seis funciones. Situar los controles de SEVEN-G en esas funciones permite que la seguridad de la IA entre en el mismo cuadro de mando y el mismo plan de acción que el resto de la ciberseguridad, sin inventar un vocabulario paralelo. Distinguir un borrador de una norma final evita decidir una puerta con un texto que aún puede cambiar.

Funciones del CSF 2.0 aplicadas a los sistemas de IA

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
Establecer, comunicar y supervisar la estrategia, las expectativas, los roles y la política de riesgo de ciberseguridad, incluidos los sistemas de IA, su uso corporativo y su cadena de suministro	GV (GV.OC, GV.RM, GV.RR, GV.PO, GV.OV, GV.SC)	Organizaciones que lo adoptan (voluntario)	C2 (política y apetito), C4 (supervisión); fase 3 (proveedores)	Consejo; alta dirección; seguridad de la información	Documentos 13, 31 y 36; 35 §9.2; P14	T19, T09, T17

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
Identificar los activos de IA (modelos, datos, conectores, identidades no humanas), sus vulnerabilidades y amenazas, y las mejoras que surgen de pruebas e incidentes	ID (ID.AM, ID.RA, ID.IM)	Ídem	Fase 0 (inventario), fase 3 (riesgos y amenazas), C5 (mejora)	Responsable técnico; Responsable de riesgos; seguridad de la información	P05, P12, P18 (modelo de amenazas, SEG-01), P54	T02, T06
Proteger identidades y accesos, formar al personal y proteger datos, plataformas e infraestructura de los sistemas de IA	PR (PR.AA, PR.AT, PR.DS, PR.PS, PR.IR)	Ídem	Fase 4 (diseño), fase 5 (pruebas); C4 (controles corporativos)	Responsable técnico; seguridad de la información	P16, P18, P54; controles SEG y AG del documento 35	T10
Detectar y analizar eventos adversos con monitorización continua de entradas, salidas, acciones y comportamiento	DE (DE.CM, DE.AE)	Ídem	Fase 6; C4	Responsable de operación; seguridad de la información	P25; SEG-12, AG-17; documento 52	T10, T08
Gestionar, analizar, comunicar y mitigar los incidentes de IA	RS (RS.MA, RS.AN, RS.CO, RS.MI)	Ídem	Fase 6 (severidades S1–S4)	Responsable de operación; seguridad de la información	P26, P27, P52; SEG-14, AG-09; documento 37	T08
Ejecutar la recuperación y comunicarla: proceso alternativo, reversión y vuelta a la operación	RC (RC.RP, RC.CO)	Ídem	Fase 6; G7 si procede	Responsable de operación	P19, P24, P26; AG-19	T08
Describir los perfiles actual y objetivo de ciberseguridad de la IA y su brecha	CSF 2.0, sección 3 (perfiles de organización)	Ídem	C1 (actual), C2 (objetivo), C5 (revisión)	Oficina de IA; seguridad de la información	P72; sección 5.5; 11 §7.5; P34	T15

Cyber AI Profile por áreas (borrador)

Área	Qué cubre	Dónde lo cubre SEVEN-G	Controles	Cobertura en la versión 0.x
Secure	Proteger los componentes de los sistemas de IA: modelos, datos, instrucciones, agentes, conectores y cadena de suministro.	35 §3–§8; riesgos tipo RT-GEN y RT-SEG del documento 33; documento 36	SEG-01 a SEG-14, SEG-26 y SEG-27; AG-01 a AG-20	Cubierta
Defend	Usar la IA en la ciberdefensa de la compañía: detección y respuesta asistidas.	35 §9.3: caso de uso con la autonomía de la respuesta fijada por tipo de acción, supervisión humana de la contención, calidad de la detección, dependencia del proveedor y pruebas del propio sistema defensivo; riesgo tipo RT-SEG-08.	SEG-21 a SEG-25; A0–A3; AG-	Cubierta
Thwart	Frustrar los ataques que usan IA: suplantación sintética, *phishing* generado, explotación acelerada.	35 §9	SEG-15 a SEG-19; SEG-13	Cubierta

La columna «Función CSF» de los catálogos SEG y AG (35 §6 y §7) indica a qué función y categoría del CSF contribuye cada control.

5.4 Perfil del AI RMF por subcategoría

La sección 5.1 mapea las 19 categorías del AI RMF. Un perfil actual u objetivo, en cambio, se construye sobre sus **72 subcategorías** (GOVERN 1.1 a MANAGE 4.3; número comprobado en la publicación NIST AI 100-1). La tabla indica, para cada una, qué pide en términos propios, dónde la cubre SEVEN-G y **de dónde sale su nivel**: la dimensión y las preguntas del cuestionario del documento 11 que lo acreditan, o «Propia» cuando ninguna pregunta la cubre y hay que evaluarla aparte. La regla de derivación está en 11 §7.5: una evaluación, dos lecturas, sin doble captura. El nivel se expresa en la escala 0–5 del documento 11; la equivalencia orientativa con los *tiers* del CSF está en 11 §2.2. Las descripciones son un resumen propio, no una traducción del texto del NIST. El perfil se documenta con la plantilla P73.

Subcategoría	Qué pide (resumen propio)	Dónde lo cubre SEVEN-G	Nivel desde el documento 11
GOVERN 1.1	Conocer, gestionar y documentar los requisitos legales y regulatorios que afectan a la IA.	Documento 34; 01 §13; P11	D6.05, D6.12 (D6)
GOVERN 1.2	Integrar las características de una IA fiable en políticas, procesos y prácticas.	Documento 31; 01 §3	D1.04 (D1)

Subcategoría	Qué pide (resumen propio)	Dónde lo cubre SEVEN-G	Nivel desde el documento 11
GOVERN 1.3	Proporcionar el nivel de gestión del riesgo a la tolerancia al riesgo de la organización.	Documento 13 (apetito); 01 §9 (intensidad); P04	D1.05, D1.06 (D1)
GOVERN 1.4	Establecer el proceso de gestión del riesgo y sus resultados con políticas y controles transparentes.	Documento 33; P12, P13	D6.04, D6.06 (D6)
GOVERN 1.5	Planificar el seguimiento continuo y la revisión periódica del proceso de riesgos, con roles y frecuencia.	33 §11; documento 30; R6	D6.09 (D6)
GOVERN 1.6	Inventariar los sistemas de IA y dotarlos de recursos según las prioridades de riesgo.	Documento 32; P05	D6.03, D6.05 (D6)
GOVERN 1.7	Retirar sistemas de IA de forma segura, sin aumentar el riesgo.	Documento 14 (retiradas); G7; P30	D2.10 (D2)
GOVERN 2.1	Documentar roles, responsabilidades y líneas de comunicación sobre el riesgo de IA.	01 §8; documento 30; P03	D1.07, D1.08 (D1)
GOVERN 2.2	Formar al personal y a los socios en gestión del riesgo de IA según su función.	Documento 50; P45	D5.05, D5.06 (D5)
GOVERN 2.3	Que la alta dirección asuma las decisiones sobre los riesgos de la IA que desarrolla o despliega.	Documentos 13 y 30; 01 §8.3	D1.05, D1.09 (D1)
GOVERN 3.1	Tomar las decisiones de riesgo con equipos diversos en disciplinas, experiencia y perfiles.	Documentos 30 y 50; P03	Propia (D5)
GOVERN 3.2	Definir los roles de la configuración persona–IA y de la supervisión de los sistemas.	P17; 35 §5; 01 §8	D6.08 (D6)
GOVERN 4.1	Fomentar el pensamiento crítico y la seguridad primero en el diseño y el uso de la IA.	Documento 31; 01 §3	Propia (D1)
GOVERN 4.2	Que los equipos documenten los riesgos e impactos de la IA y los comuniquen.	P11, P12; documento 33	D6.06 (D6)
GOVERN 4.3	Permitir las pruebas de la IA, la identificación de incidentes y el intercambio de información.	Documento 37; 35 §8; P26, P53	D6.07, D6.10 (D6)
GOVERN 5.1	Recoger y tener en cuenta la opinión externa sobre los impactos individuales y sociales.	P11, P46, P48	Propia (D6)
GOVERN 5.2	Incorporar al diseño la retroalimentación ya valorada de los actores relevantes.	Documento 20; P27	Propia (D2)

Subcategoría	Qué pide (resumen propio)	Dónde lo cubre SEVEN-G	Nivel desde el documento 11
GOVERN 6.1	Tratar los riesgos de terceros, incluida la infracción de propiedad intelectual u otros derechos.	Documento 36; P14, P55, P56	D6.08 (D6)
GOVERN 6.2	Tener contingencias ante fallos o incidentes de datos o sistemas de terceros de alto riesgo.	Documento 36; P19, P57	D6.08 (D6)
MAP 1.1	Documentar la finalidad, los usos, las normas aplicables y el entorno de despliegue.	P01, P02	D2.05 (D2)
MAP 1.2	Contar con actores interdisciplinares y diversos al fijar el contexto.	P03; documento 30	Propia (D5)
MAP 1.3	Conocer y documentar la misión y los objetivos de la organización para la IA.	Documento 13 (tesis)	D1.05 (D1)
MAP 1.4	Definir, o reevaluar en sistemas existentes, el valor de negocio.	P07, P08; documento 40	D2.08 (D2)
MAP 1.5	Determinar y documentar las tolerancias al riesgo.	Documento 13 (apetito); P35	D1.05, D1.06 (D1)
MAP 1.6	Recoger los requisitos del sistema teniendo en cuenta sus implicaciones sociotécnicas.	P15, P17	Propia (D4)
MAP 2.1	Definir las tareas y los métodos del sistema (clasificador, generativo, recomendador…).	P05, P15	D6.05 (D6)
MAP 2.2	Documentar los límites de conocimiento del sistema y cómo se usan y supervisan sus salidas.	P17, P49	Propia (D6)
MAP 2.3	Documentar la integridad científica y las pruebas: diseño, selección de datos, validez.	P09, P16, P22; documento 51	D3.04, D3.07 (D3)
MAP 3.1	Examinar y documentar los beneficios esperados.	P08; documento 40	D2.08 (D2)
MAP 3.2	Examinar los costes, también no monetarios, de los errores del sistema.	P10, P12; documento 42	D6.06 (D6)
MAP 3.3	Delimitar el alcance de la aplicación según su capacidad, contexto y categoría.	P01, P02, P15	D2.05 (D2)
MAP 3.4	Definir y evaluar la competencia de operadores y profesionales.	Documento 50; P20, P45	D5.05, D5.06 (D5)
MAP 3.5	Definir y documentar la supervisión humana.	P17; 35 §4.6	D4.06 (D4)

Subcategoría	Qué pide (resumen propio)	Dónde lo cubre SEVEN-G	Nivel desde el documento 11
MAP 4.1	Identificar los riesgos tecnológicos y legales de los componentes, incluidos los de terceros.	P11, P14; documento 36	D6.08 (D6)
MAP 4.2	Documentar los controles internos sobre los componentes, incluidos los de terceros.	P13, P18; SEG-09	D6.08 (D6)
MAP 5.1	Estimar la probabilidad y la magnitud de cada impacto identificado.	P11, P12; documento 33	D6.06 (D6)
MAP 5.2	Mantener la relación con los actores relevantes e integrar su opinión sobre los impactos.	P25, P28; documento 52	Propia (D6)
MEASURE 1.1	Elegir métodos y métricas para los riesgos más significativos y documentar lo que no se mide.	P09, P22; documento 41	D7.03 (D7)
MEASURE 1.2	Revisar la idoneidad de las métricas y la eficacia de los controles.	Documento 41; R6; P28	D7.09; D6 · D6.11 (D7)
MEASURE 1.3	Implicar a evaluadores internos no participantes o externos en las evaluaciones.	Documento 38; 01 §8.2	D6.10 (D6)
MEASURE 2.1	Documentar conjuntos de prueba, métricas y herramientas de evaluación.	P22; documento 53	D4.08 (D4)
MEASURE 2.2	Que las evaluaciones con personas cumplan sus requisitos y sean representativas.	P22	Propia (D6)
MEASURE 2.3	Medir el rendimiento en condiciones parecidas a las de uso real.	P09, P22	D4.08 (D4)
MEASURE 2.4	Monitorizar el funcionamiento del sistema en producción.	P25; documento 52	D4.05, D4.09 (D4)
MEASURE 2.5	Demostrar la validez y fiabilidad, y documentar los límites de generalización.	P22; G5	D4.08 (D4)
MEASURE 2.6	Evaluar la seguridad del sistema frente a daños y su capacidad de fallar de forma segura.	P19, P22; AG-09	D4.06 (D4)
MEASURE 2.7	Evaluar y documentar la seguridad frente a ataques y la resiliencia.	P18, P53; 35 §8	D6.10 (D6)
MEASURE 2.8	Examinar los riesgos de transparencia y de rendición de cuentas.	P17, P49; P03	Propia (D6)
MEASURE 2.9	Explicar el modelo e interpretar sus salidas en su contexto.	P17, P21	Propia (D4)

Subcategoría	Qué pide (resumen propio)	Dónde lo cubre SEVEN-G	Nivel desde el documento 11
MEASURE 2.10	Examinar y documentar el riesgo para la privacidad.	P11, P47; documento 51	D3.06 (D3)
MEASURE 2.11	Evaluar la equidad y el sesgo y documentar los resultados.	P22; 52 §4.2.7	Propia (D6)
MEASURE 2.12	Evaluar el impacto ambiental del entrenamiento y la operación.	Documento 42; P10	Propia (D4)
MEASURE 2.13	Evaluar la eficacia de las propias métricas y procesos de prueba.	Documento 41; C5	Propia (D7)
MEASURE 3.1	Identificar y seguir los riesgos existentes, imprevistos y emergentes.	33 §11; P12; R6	D6.09 (D6)
MEASURE 3.2	Seguir los riesgos que aún no pueden medirse con las técnicas disponibles.	Documento 33; P12	Propia (D6)
MEASURE 3.3	Dar a usuarios y afectados un cauce para comunicar problemas y recurrir resultados.	P17, P24, P49; documento 37	Propia (D6)
MEASURE 4.1	Conectar la medición al contexto de uso con la opinión de expertos y usuarios.	P09, P22	Propia (D7)
MEASURE 4.2	Validar con expertos y actores relevantes los resultados sobre la fiabilidad en uso.	P28; R6	D7.09 (D7)
MEASURE 4.3	Identificar mejoras o empeoramientos medibles del rendimiento y la fiabilidad.	P28; documento 41	D2.10; D7 · D7.09 (D2)
MANAGE 1.1	Decidir si el sistema cumple su finalidad y si su desarrollo o despliegue debe continuar.	Documento 21; P29	D2.06 (D2)
MANAGE 1.2	Priorizar el tratamiento de los riesgos por impacto, probabilidad y recursos.	P13; 33 §7	D6.06 (D6)
MANAGE 1.3	Planificar la respuesta a los riesgos altos: mitigar, transferir, evitar o aceptar.	P13; 33 §7	D6.06 (D6)
MANAGE 1.4	Documentar los riesgos residuales para usuarios y adquirentes.	P12, P13	D6.06 (D6)
MANAGE 2.1	Considerar los recursos necesarios y las alternativas sin IA.	P06, P10; 01 §6.3	D2.08 (D2)
MANAGE 2.2	Mantener el valor de los sistemas desplegados.	R6; P28; documento 43	D2.10 (D2)

Subcategoría	Qué pide (resumen propio)	Dónde lo cubre SEVEN-G	Nivel desde el documento 11
MANAGE 2.3	Responder y recuperarse cuando aparece un riesgo desconocido.	Documento 37; P26	D6.07 (D6)
MANAGE 2.4	Poder sustituir, desenganchar o desactivar un sistema que se aparta de su uso previsto.	P19; AG-09; T22	D4.06 (D4)
MANAGE 3.1	Seguir los riesgos y beneficios de los recursos de terceros.	Documento 36; P57	D6.08 (D6)
MANAGE 3.2	Seguir los modelos preentrenados como parte de la monitorización.	P25, P54; SEG-09	D4.08 (D4)
MANAGE 4.1	Aplicar planes de seguimiento tras el despliegue: opinión de usuarios, recurso, anulación, retirada, incidentes y cambios.	P24, P25, P27; documento 52	D4.05, D4.07 (D4)
MANAGE 4.2	Integrar la mejora continua en las actualizaciones del sistema.	P28; R6; C5	D4.12 (D4)
MANAGE 4.3	Comunicar y gestionar los incidentes y errores, también a las comunidades afectadas.	Documento 37; P26, P27, P51	D6.07 (D6)

5.5 Perfil de seguridad de la IA: subcategorías del CSF 2.0

El perfil de seguridad de la IA se construye sobre las subcategorías del CSF 2.0. La tabla recoge las **48** a las que el Cyber AI Profile propone **prioridad alta (1)** en al menos una de sus tres áreas, con la prioridad que propone en cada una (**S** Secure · **D** Defend · **T** Thwart; 1 alta, 2 moderada, 3 fundamental). **La selección es provisional** mientras el perfil sea un borrador (sección 5.3) y se revisará cuando el NIST publique una versión posterior. Las demás subcategorías del CSF pueden añadirse al perfil de la compañía si su contexto lo pide. Como en la sección 5.4, el nivel se deriva del documento 11 (11 §7.5) y las descripciones son un resumen propio. El perfil se documenta con la plantilla P72.

Subcategoría	Qué pide (resumen propio)	Prioridad S · D · T	Dónde lo cubre SEVEN-G	Nivel desde el documento 11
GV.OC-03	Conocer y gestionar los requisitos legales, regulatorios y contractuales de ciberseguridad, incluida la privacidad.	3 · 1 · 3	Documento 34; P11, P56	D6.05, D6.12 (D6)
GV.OC-04	Conocer y comunicar los objetivos y servicios críticos de los que dependen terceros.	1 · 1 · 3	P02; 01 §9.2 (función crítica); P49	Propia (D4)

Subcategoría	Qué pide (resumen propio)	Prioridad S · D · T	Dónde lo cubre SEVEN-G	Nivel desde el documento 11
GV.OC-05	Conocer y comunicar los resultados y servicios de los que depende la organización, incluidos los que aporta la IA.	1 · 2 · 3	P02, P15; documento 36	Propia (D4)
GV.RM-02	Fijar, comunicar y mantener el apetito y la tolerancia al riesgo.	2 · 2 · 1	Documento 13; P35	D1.05 (D1)
GV.RM-07	Incluir las oportunidades estratégicas en las conversaciones sobre el riesgo.	3 · 1 · 3	Documentos 13 y 14; P06	D2.07 (D2)
GV.RR-01	Que la dirección responda del riesgo y promueva una cultura consciente del riesgo.	3 · 1 · 2	Documentos 13 y 30; P38	D1.01, D1.09 (D1)
GV.RR-02	Establecer y hacer cumplir roles, responsabilidades y autoridades de gestión del riesgo.	3 · 1 · 2	01 §8; documento 30; P03	D1.07, D1.08 (D1)
GV.RR-03	Asignar recursos proporcionados a la estrategia de riesgo.	2 · 2 · 1	Documentos 13 y 14; P36	Propia (D1)
GV.RR-04	Incluir la ciberseguridad en las prácticas de recursos humanos.	1 · 3 · 1	Documento 50; P45, P46	Propia (D5)
GV.PO-01	Establecer, comunicar y hacer cumplir la política de gestión del riesgo.	3 · 1 · 3	Documentos 31 y 35	D1.04 (D1)
GV.PO-02	Revisar y actualizar la política ante cambios de requisitos, amenazas o tecnología.	1 · 1 · 2	Documento 31; C5; P37	D6.12 (D6)
GV.SC-03	Integrar el riesgo de la cadena de suministro en la gestión del riesgo.	1 · 2 · 3	Documentos 33 y 36	D6.08 (D6)
GV.SC-07	Conocer, evaluar y seguir el riesgo de cada proveedor durante toda la relación.	1 · 1 · 3	Documento 36; P14, P55, P57	D6.08 (D6)
ID.AM-03	Mantener la representación de las comunicaciones y los flujos de datos autorizados.	1 · 2 · 2	P15, P16	D3.07 (D3)
ID.AM-07	Mantener inventarios de datos y de sus metadatos.	1 · 1 · 3	P64; documento 51	D3.03, D3.05 (D3)
ID.AM-08	Gestionar sistemas, software, servicios y datos durante todo su ciclo de vida.	1 · 3 · 2	Documento 20; P05, P54	D6.05 (D6)

Subcategoría	Qué pide (resumen propio)	Prioridad S · D · T	Dónde lo cubre SEVEN-G	Nivel desde el documento 11
ID.RA-01	Identificar, validar y registrar las vulnerabilidades de los activos.	1 · 1 · 1	SEG-11, SEG-13, SEG-19; P53	D6.10 (D6)
ID.RA-03	Identificar y registrar las amenazas internas y externas.	1 · 1 · 1	SEG-01; P18; 35 §3 y §9	D6.08 (D6)
ID.RA-04	Estimar el impacto y la probabilidad de que una amenaza explote una vulnerabilidad.	1 · 1 · 1	P12; documento 33	D6.06 (D6)
ID.RA-06	Elegir, priorizar, planificar, seguir y comunicar las respuestas al riesgo.	3 · 2 · 1	P13; 33 §7	D6.06 (D6)
ID.RA-07	Gestionar y registrar los cambios y excepciones, evaluando su efecto en el riesgo.	2 · 1 · 1	P27, P40; documento 52	D4.04 (D4)
ID.RA-08	Recibir, analizar y responder a las divulgaciones de vulnerabilidades.	3 · 3 · 1	SEG-13; documento 37	Propia (D6)
PR.AA-01	Gestionar las identidades y credenciales de usuarios, servicios y agentes.	1 · 2 · 1	AG-01, AG-03; P54	D6.08 (D6)
PR.AA-05	Definir y revisar los permisos con mínimo privilegio y separación de funciones.	1 · 2 · 1	AG-02, AG-20; SEG-06	D6.08 (D6)
PR.AT-01	Concienciar y formar al personal para trabajar teniendo en cuenta el riesgo.	1 · 1 · 1	Documento 50; SEG-17; P45	D5.05 (D5)
PR.AT-02	Formar a quienes ocupan roles especializados.	2 · 1 · 1	Documento 50; P45	D5.06 (D5)
PR.DS-01	Proteger la confidencialidad, integridad y disponibilidad de los datos almacenados.	1 · 1 · 2	SEG-07, SEG-08; P16, P18	D3.05 (D3)
PR.DS-10	Proteger los datos en uso (contexto, instrucciones, memoria).	1 · 1 · 3	SEG-05, SEG-06, SEG-07; AG-14	Propia (D6)
PR.PS-01	Establecer y aplicar la gestión de la configuración.	1 · 1 · 3	P15, P27; documento 52	D4.04 (D4)
PR.PS-02	Mantener, sustituir y retirar el software según el riesgo.	3 · 3 · 1	SEG-09, SEG-13; P54	Propia (D4)
PR.PS-03	Mantener, sustituir y retirar el hardware según el riesgo.	3 · 2 · 1	Documento 52	Propia (D4)

Subcategoría	Qué pide (resumen propio)	Prioridad S · D · T	Dónde lo cubre SEVEN-G	Nivel desde el documento 11
PR.PS-04	Generar registros disponibles para la monitorización continua.	1 · 1 · 1	AG-10, SEG-12; P25	D4.08 (D4)
PR.PS-05	Impedir la instalación y ejecución de software no autorizado, también de IA.	2 · 2 · 1	SEG-20, AG-13; documento 31; T21	D6.09 (D6)
PR.IR-01	Proteger redes y entornos frente a accesos y usos no autorizados.	2 · 2 · 1	AG-11; P15	D4.03 (D4)
PR.IR-03	Aplicar mecanismos de resiliencia en situaciones normales y adversas.	2 · 1 · 2	P19; AG-16; documento 52	D4.06, D4.12 (D4)
DE.CM-01	Monitorizar redes y servicios de red para detectar eventos adversos.	2 · 1 · 1	SEG-12	Propia (D4)
DE.CM-06	Monitorizar la actividad de los proveedores de servicios externos.	1 · 2 · 2	Documento 36; P57	D6.08 (D6)
DE.CM-09	Monitorizar hardware, software, entornos de ejecución y datos.	1 · 1 · 2	SEG-12, AG-17; P25	D4.05 (D4)
DE.AE-03	Correlacionar información de varias fuentes.	3 · 1 · 2	SEG-12	Propia (D4)
DE.AE-04	Entender el impacto y el alcance estimados de los eventos adversos.	3 · 1 · 2	Documento 37; P27	D6.07 (D6)
DE.AE-06	Hacer llegar la información de eventos adversos a las personas y herramientas autorizadas.	3 · 2 · 1	P24, P25	D4.05 (D4)
DE.AE-07	Integrar la inteligencia de amenazas en el análisis.	3 · 2 · 1	35 §9; SEG-19	Propia (D6)
RS.MA-02	Clasificar y validar las notificaciones de incidentes.	2 · 1 · 2	Documento 37; P27	D6.07 (D6)
RS.MA-03	Categorizar y priorizar los incidentes.	2 · 1 · 1	Documento 37 (S1–S4); P27	D6.07 (D6)
RS.AN-03	Analizar lo ocurrido en un incidente y su causa raíz.	1 · 1 · 1	P52; documento 37	D6.07 (D6)
RS.AN-06	Registrar las acciones de la investigación preservando su integridad y procedencia.	3 · 3 · 1	P27, P52	D6.07 (D6)

Subcategoría	Qué pide (resumen propio)	Prioridad S · D · T	Dónde lo cubre SEVEN-G	Nivel desde el documento 11
RS.AN-07	Recoger los datos del incidente preservando su integridad y procedencia.	1 · 2 · 2	AG-10; P27	D4.08 (D4)
RC.RP-02	Seleccionar, delimitar, priorizar y ejecutar las acciones de recuperación.	3 · 1 · 3	P19, P24, P26; AG-19	D4.06 (D4)

06

RGPD y guías del CEPD

6.1 Artículos del RGPD

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
Principios: licitud, lealtad y transparencia; limitación de la finalidad; minimización; exactitud; limitación del plazo de conservación; integridad y confidencialidad; responsabilidad proactiva	Art. 5	Responsables y encargados del tratamiento	Fases 3–4; verificación en G3 y G4	Responsable de riesgos; delegado de protección de datos (asesora)	P11, P16	T07
Base jurídica del tratamiento en entrenamiento, prueba y uso	Art. 6	Responsables del tratamiento	Fase 3	Responsable de riesgos; asesoría jurídica	P11, P16	T07

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
Condiciones para tratar categorías especiales de datos, incluido el tratamiento para detectar y corregir sesgos permitido por el Reglamento de IA	Art. 9; Reglamento de IA, arts. 4 bis y 10	Responsables del tratamiento	Fases 3–5	Responsable de riesgos; delegado de protección de datos	P11, P16	T07
Información a los interesados, incluida la existencia de decisiones automatizadas e información significativa sobre la lógica aplicada	Arts. 13.2.f y 14.2.g	Responsables del tratamiento	Fase 4 (diseño), fase 6	Responsable de producto	P17, P24	—
Derecho de acceso, incluida la información sobre decisiones automatizadas	Art. 15.1.h	Responsables del tratamiento	Fase 6	Responsable de operación; delegado de protección de datos	P24, P27	T08
No sujeción a decisiones basadas únicamente en tratamiento automatizado con efectos jurídicos o significativos, salvo excepciones con garantías (intervención humana, expresar el punto de vista, impugnar)	Art. 22	Responsables del tratamiento	Fase 3 (clasificación), fase 4 (supervisión humana), fase 6	Responsable de producto; Responsable de riesgos	P11, P17	T07
Protección de datos desde el diseño y por defecto	Art. 25	Responsables del tratamiento	Fase 4; verificado en G4	Responsable técnico	P15, P16, P18	T10
Registro de actividades de tratamiento	Art. 30	Responsables y encargados	Fase 4, antes de G5	Delegado de protección de datos; Responsable técnico	P16, P23	T02

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
Notificación de violaciones de seguridad a la autoridad de control en 72 horas y, si hay alto riesgo, a los interesados	Arts. 33 y 34	Responsables del tratamiento	Fase 6 (S1–S2)	Responsable de operación; delegado de protección de datos	P26, P27	T08
Evaluación de impacto relativa a la protección de datos cuando sea probable un alto riesgo (en particular, evaluación sistemática y exhaustiva basada en tratamiento automatizado) y consulta previa si procede	Arts. 35 y 36	Responsables del tratamiento	Fase 3; actualizada en 4 y R6	Responsable de riesgos; delegado de protección de datos (asesora y supervisa)	P11, P47	T07

6.2 Guías del CEPD y jurisprudencia relevantes para IA

Referencia	Fecha	Estado	Uso en SEVEN-G
Directrices sobre decisiones individuales automatizadas y elaboración de perfiles (WP251 rev.01, asumidas por el CEPD)	2018	Vigentes	P11, P17
Directrices sobre la evaluación de impacto relativa a la protección de datos (WP248 rev.01, asumidas por el CEPD)	2017	Vigentes	P11
Directrices 4/2019 sobre el art. 25 (protección de datos desde el diseño y por defecto)	2020 (versión 2.0)	Vigentes	P15, P18
Declaración 3/2024 sobre el papel de las autoridades de protección de datos en el marco del Reglamento de IA	Julio de 2024	Publicada	Sección 8
Dictamen 28/2024 sobre aspectos de protección de datos en el tratamiento de datos personales en modelos de IA (anonimato de modelos, interés legítimo, efectos del tratamiento ilícito)	Diciembre de 2024	Publicado	P11, P14, P16

Referencia	Fecha	Estado	Uso en SEVEN-G
Directrices 01/2025 sobre seudonimización	Enero de 2025	Versión final pendiente de confirmar	P16
Directrices 02/2026 sobre anonimización y Directrices 03/2026 sobre extracción web en el contexto de la IA generativa	Adoptadas en julio de 2026	En consulta pública hasta el 30-10-2026	P14, P16
Sentencia del TJUE C-634/21 (SCHUFA): la puntuación que condiciona decisiones de terceros puede ser decisión automatizada del art. 22	7-12-2023	Firme	P11 (sistemas de puntuación)
Sentencia del TJUE C-203/22 (Dun & Bradstreet Austria) sobre el alcance de la información significativa de la lógica aplicada	27-02-2025	Firme	P17, P24

Propuesta de modificación del RGPD. El paquete ómnibus digital de noviembre de 2025 incluye, además de la parte de IA ya adoptada, una propuesta que modifica el RGPD (COM(2025) 837 final; procedimiento 2025/0360(COD)) (entre otros aspectos, definición de dato personal, interés legítimo para el desarrollo de IA y notificación de violaciones). A fecha de consulta, esa parte **sigue en tramitación y no está adoptada**; su contenido final está pendiente de confirmar. No se aplica en este mapeo.

07

DORA y NIS2

Solo aplican a las compañías incluidas en su ámbito: DORA a las entidades financieras del art. 2 del Reglamento (UE) 2022/2554, aplicable desde el 17-01-2025; NIS2 a las entidades esenciales e importantes definidas en la Directiva (UE) 2022/2555 y en su transposición nacional. Si aplican, un sistema de IA que soporta una función crítica o importante es criterio Enterprise (01 §9.2).

7.1 DORA

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
Responsabilidad del órgano de dirección sobre el riesgo TIC	Art. 5	Entidades financieras	C2, C4	Consejo; comisión delegada	Documentos 13 y 60	T17
Marco de gestión del riesgo TIC que incluya los sistemas de IA	Art. 6	Entidades financieras	C2; fases 3–6	Segunda línea; Responsable de riesgos	Documentos 33 y 35; P12	T06
Identificación, protección, detección, respuesta y recuperación, copias de seguridad, aprendizaje	Arts. 8 a 13	Entidades financieras	Fases 4–6	Responsable técnico; Responsable de operación	P15, P18, P19, P24, P25, P26	T10
Proceso de gestión, clasificación y notificación de incidentes graves relacionados con las TIC, con los plazos de sus normas técnicas	Arts. 17 a 19	Entidades financieras	Fase 6	Responsable de operación; segunda línea	P26, P27; documento 37	T08
Pruebas de resiliencia operativa digital	Arts. 24 a 27	Entidades financieras (pruebas avanzadas solo las designadas)	Fase 5; C4	Responsable técnico; seguridad de la información	P22	T10
Gestión del riesgo de terceros proveedores TIC, registro de información y evaluación del riesgo de concentración	Arts. 28 y 29	Entidades financieras	Fase 3; C4	Responsable de riesgos	P14; documento 36	T09
Cláusulas contractuales esenciales con proveedores TIC (incluidos proveedores de modelos y plataformas de IA)	Art. 30	Entidades financieras	Fases 3–4	Responsable de riesgos; asesoría jurídica	P14; documento 36	T09

7.2 NIS2

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
Aprobación y supervisión de las medidas de ciberseguridad por los órganos de dirección y formación de sus miembros	Art. 20	Entidades esenciales e importantes	C2, C4	Consejo; alta dirección	Documentos 13, 35 y 60	T17
Medidas de gestión de riesgos de ciberseguridad, incluida la seguridad de la cadena de suministro	Art. 21 (en particular 21.2.d)	Entidades esenciales e importantes	Fases 3–6	Seguridad de la información; Responsable técnico	P14, P18; documento 35	T09, T10
Notificación de incidentes significativos: alerta temprana en 24 horas, notificación en 72 horas e informe final en un mes	Art. 23	Entidades esenciales e importantes	Fase 6 (S1–S2)	Responsable de operación; seguridad de la información	P26, P27	T08

Transposición en España. A fecha de consulta, la ley que transpone NIS2 (Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad , aprobado en primera vuelta en enero de 2025) **no ha sido remitida a las Cortes Generales ni publicada en el BOE** (Departamento de Seguridad Nacional; BOE). El 8-07-2026 la Comisión Europea llevó a España ante el Tribunal de Justicia de la UE por no haber notificado la transposición (comunicado IP/26/1499).

Productos con elementos digitales. Si la compañía fabrica productos con elementos digitales que incorporan IA, debe valorarse además el Reglamento (UE) 2024/2847 de ciberresiliencia (obligaciones de notificación del art. 14 desde el 11-09-2026 y obligaciones principales desde el 11-12-2027). El documento 35 lo recoge en sus referencias y en los controles SEG-13 y SEG-14.

08

Normativa española y AESIA

8.1 Estado a fecha de consulta

Norma o actuación	Referencia	Estado a 16-09-2026
Estatuto de la Agencia Española de Supervisión de Inteligencia Artificial (AESIA)	Real Decreto 729/2023 , de 22 de agosto (BOE-A-2023-18911)	Vigente. AESIA actúa como autoridad de vigilancia del mercado y punto de contacto único.
Entorno controlado de pruebas para el ensayo del cumplimiento del Reglamento de IA	Real Decreto 817/2023 , de 8 de noviembre (BOE-A-2023-22767)	Vigente. El Gobierno comunicó la conclusión del primer entorno de pruebas en junio de 2026; nuevas convocatorias pendientes de confirmar.
Guías de apoyo al cumplimiento del Reglamento de IA	AESIA, 16-12-2025: dos guías introductorias, trece guías de requisitos técnicos y listas de verificación, derivadas del entorno de pruebas	Publicadas; no vinculantes.
Proyecto de Ley Orgánica para el buen uso y la gobernanza de la inteligencia artificial	Aprobado por el Consejo de Ministros el 26-05-2026; BOCG, Congreso, serie A, núm. 97-1, de 12-06-2026; expediente 121/000096	**En tramitación**: fase de enmiendas en la Comisión de Economía, Comercio y Transformación Digital, con plazo ampliado sucesivamente (última ampliación conocida hasta el 23-09-2026). Contenido final y fecha de aprobación pendientes.
Instrucción 2/2026 del CGPJ sobre la utilización de sistemas de IA en la actividad jurisdiccional	BOE-A-2026-2205	Publicada. Solo relevante para el ámbito judicial.
Normativa autonómica	Por ejemplo, Ley 2/2025, de 2 de abril, para el desarrollo e impulso de la IA en Galicia	Vigente en su ámbito; revisar según la implantación territorial de la compañía.
Guías de la AEPD sobre tratamientos que incorporan IA y auditoría de esos tratamientos	AEPD	Publicadas; referencia para P11.

Según el proyecto publicado en el Boletín Oficial de las Cortes Generales, la ley designaría autoridades de vigilancia del mercado, un régimen de infracciones leves, graves y muy graves, reglas para el sector

público y regulación de los espacios controlados de pruebas. **Todo ello está pendiente de confirmar en el texto que finalmente se apruebe.**

8.2 Mapeo

Obligación / requisito	Artículo o cláusula	A quién aplica	Fase o etapa SEVEN-G	Rol responsable	Evidencia (P-código o documento)	Herramienta
Identificar la autoridad de vigilancia del mercado competente para cada sistema (AESIA o autoridad sectorial)	RD 729/2023; proyecto de ley orgánica (pendiente)	Proveedores y responsables del despliegue en España	Fase 3	Responsable de riesgos; asesoría jurídica	P11	T07
Canalizar notificaciones de incidentes graves y de evaluaciones de impacto en derechos fundamentales a la autoridad competente	Reglamento de IA arts. 27.3 y 73; normativa nacional pendiente	Proveedores y responsables del despliegue	Fases 5–6	Responsable de riesgos	P11, P26, P27	T08
Valorar la participación en un entorno controlado de pruebas cuando el caso de uso sea de alto riesgo y la viabilidad regulatoria sea incierta	RD 817/2023; Reglamento de IA arts. 57–59	Proveedores y responsables del despliegue	Fase 3 (decisión), fases 4–5 (ejecución)	Patrocinador; Responsable de riesgos	P10, P13	T01
Usar las guías de AESIA como referencia de los requisitos técnicos	Guías AESIA (diciembre de 2025)	Proveedores y responsables del despliegue	Fases 3–6	Responsable técnico; Responsable de riesgos	P11, P15, P18, P22	T07, T03
Vigilar la tramitación de la ley orgánica y actualizar este mapeo cuando se publique en el BOE	Expediente 121/000096	Oficina de IA	Sección 10	Oficina de IA; asesoría jurídica	Documento 34	T07

09

Matriz resumen: etapas y fases × referencias

Lectura: qué pide cada referencia en cada etapa del ciclo corporativo y en cada fase del ciclo de vida. "—" indica que no hay obligación principal en ese punto.

Etapa o fase	Reglamento de IA	ISO/IEC 42001	NIST AI RMF / 600-1 · CSF 2.0	RGPD	DORA / NIS2 (si aplican)	Normativa española
Diagnóstico (C1)	Inventario y rol por sistema (arts. 3, 25)	4.1, 4.2	MAP 1 · ID.AM, GV.OC; perfil actual	Registro de tratamientos existente (art. 30)	Inventario TIC y registro de terceros (DORA art. 28)	Autoridades competentes identificadas
Dirección (C2)	Alfabetización (art. 4); política frente a prácticas prohibidas	4.3, 5.1–5.3, 6.1–6.2, A.2, A.3	GOVERN 1–4 · GV.RM, GV.RR, GV.PO; perfil objetivo	Responsabilidad proactiva (art. 5.2)	Responsabilidad del órgano de dirección (DORA art. 5; NIS2 art. 20)	—
Cartera (C3)	Señales de alto riesgo en la cartera	6.3, 7.1–7.2	GOVERN 2, 6 · GV.SC	—	Riesgo de concentración (DORA art. 29)	—
Supervisión (C4)	Incidentes graves y vigilancia agregada	9.1, 9.2	MEASURE 3–4 · GV.OV, DE.CM	Violaciones de seguridad (arts. 33–34)	Incidentes graves (DORA arts. 17–19; NIS2 art. 23)	Seguimiento de la ley orgánica
Revisión (C5)	Revisión del mapeo y de las clasificaciones	9.3, 10.1, 10.2	MEASURE 4; MANAGE 4 · ID.IM; revisión del perfil	—	Aprendizaje (DORA art. 13)	—
0 · Contexto	Ámbito, rol y clasificación provisional	5.3, 8.1	MAP 1 · ID.AM	Identificar si hay datos personales	Identificar si soporta función crítica	Posible entorno de pruebas
1 · Descubrimiento	Filtrado de prácticas prohibidas y señales del anexo III	A.9	MAP 1, MAP 3	—	—	—
2 · Hipótesis	—	6.2	MAP 3; MEASURE 1	Minimización y finalidad (art. 5)	—	—

Etapa o fase	Reglamento de IA	ISO/IEC 42001	NIST AI RMF / 600-1 · CSF 2.0	RGPD	DORA / NIS2 (si aplican)	Normativa española
3 · Viabilidad y riesgo	Clasificación (arts. 5, 6, 50); gestión de riesgos (art. 9); evaluación de impacto en derechos fundamentales (art. 27); modelos de uso general (art. 53)	6.1.2–6.1.4, 8.2–8.4, A.5, A.7, A.10	MAP 2–5; GOVERN 6; riesgos de 600-1 · ID.RA, GV.SC	Base jurídica (arts. 6, 9); evaluación de impacto (art. 35); art. 22	Riesgo de terceros y contratos (DORA arts. 28–30; NIS2 art. 21)	Autoridad competente; guías AESIA
4 · Diseño	Datos (art. 10), documentación (art. 11), registros (art. 12), instrucciones (art. 13), supervisión humana (art. 14), ciberseguridad (art. 15), transparencia (art. 50)	8.1, A.4, A.6, A.7, A.8	MANAGE 2; controles de 600-1 · PR.AA, PR.DS, PR.PS	Protección de datos desde el diseño (art. 25); información (arts. 13–14)	Protección y detección (DORA arts. 8–10)	Guías AESIA
5 · Entrega y validación	Pruebas (arts. 9, 15), conformidad, declaración y marcado CE (arts. 43, 47, 48), registro (art. 49), información a trabajadores (art. 26.7), notificación de la evaluación de impacto (art. 27.3)	A.6, A.8	MEASURE 1–2 · ID.IM (pruebas)	Registro de tratamientos actualizado (art. 30)	Pruebas de resiliencia (DORA arts. 24–27)	Notificaciones a la autoridad competente

Etapa o fase	Reglamento de IA	ISO/IEC 42001	NIST AI RMF / 600-1 · CSF 2.0	RGPD	DORA / NIS2 (si aplican)	Normativa española
6 · Operación	Obligaciones del responsable del despliegue (art. 26), vigilancia posterior a la comercialización (art. 72), incidentes graves (art. 73), explicación (art. 86)	8.2–8.4, 9.1, A.6, A.8	MEASURE 3; MANAGE 1, 4 · DE, RS, RC	Derechos (arts. 15, 22); violaciones (arts. 33–34)	Incidentes y recuperación (DORA arts. 11, 17–19; NIS2 art. 23)	Notificaciones y requerimientos
7 · Evolución o retirada	Medidas correctoras y retirada (art. 20); conservación de documentación (art. 18); actualización del registro (art. 49)	10.1, 10.2	MANAGE 2, 4 · RC.RP; PR.AA (revocación)	Conservación y supresión de datos (art. 5.1.e)	Estrategia de salida del proveedor (DORA art. 28)	—

9.1 Crosswalk de cobertura: normas y regulación × SEVEN-G

La matriz anterior dice qué pide cada referencia en cada momento. El crosswalk responde a la pregunta inversa, la que hace un auditor o un comité que ya trabaja con una norma: **para cada requisito, dónde lo cubre SEVEN-G, con qué regla del núcleo (01 §14.1), con qué evidencia y hasta dónde**. Cubre ISO/IEC 42001 , ISO/IEC 38507 , ISO/IEC 23894 , ISO/IEC 42005, el NIST AI RMF y el Reglamento Europeo de IA .

Escala de cobertura

Cobertura	Qué significa
Directa	SEVEN-G pide lo que el requisito exige, con su evidencia.
Parcial	SEVEN-G cubre una parte; la nota dice qué falta y quién lo completa.
Requiere control externo	El requisito lo cumple un tercero o un procedimiento fuera del marco (por ejemplo, la certificación o el marcado CE); SEVEN-G solo lo sitúa.
No cubierto	SEVEN-G no lo trata; se cita para que la compañía no dé por hecho que sí.

> **Por qué importa.** Una compañía que ya tiene un sistema de gestión ISO o que trabaja con el NIST no adopta un marco nuevo si no ve dónde encaja con lo que ya hace. El crosswalk le dice qué reutiliza, qué completa y qué tiene que buscar fuera, sin que nadie lo reconstruya a mano en cada auditoría.

Cómo se lee y sus límites. Las normas ISO se citan por el número de su apartado o, cuando su numeración no se ha podido cotejar en una fuente oficial abierta, **por tema**; el texto de cada fila es un **resumen propio**, nunca el de la norma, que debe cotejarse con el texto adquirido. El crosswalk **no es una certificación, una declaración de conformidad ni asesoramiento jurídico** (D25): sirve para orientar una auditoría o un análisis de brechas. Las tablas se generan desde un único fichero de datos versionado (`SEVEN-G/build/crosswalk/crosswalk.json`) con la versión del núcleo a la que corresponden; si cambia el núcleo o una norma, se actualiza ese fichero y se vuelve a generar.

Generado desde `crosswalk.json` (versión 1, 01-10-2026; versión del núcleo 1). No se edita a mano.

Norma	Filas	Directa	Parcial	Requiere control externo	No cubierto
ISO/IEC 42001:2023 · Sistema de gestión de la IA	17	14	2	1	0
ISO/IEC 38507:2022 · Gobierno de la IA por el órgano de gobierno	6	5	1	0	0
ISO/IEC 23894:2023 · Gestión del riesgo de la IA	6	6	0	0	0
ISO/IEC 42005:2025 · Evaluación del impacto de los sistemas de IA	5	4	1	0	0
NIST AI RMF 1.0	4	4	0	0	0
Reglamento (UE) 2024/1689 (Reglamento Europeo de IA)	14	8	2	2	2
Total	52	41	6	3	2

ISO/IEC 42001:2023 · Sistema de gestión de la IA

Ref.	Tema (resumen propio)	Núcleo	Dónde en SEVEN-G	Evidencia	Cobertura	Nota
4.1	Contexto de la organización y su papel respecto a la IA	N-01, N-12	01 §5 (C1); 11; 32	P33; T02, T15	Directa	—
4.2	Partes interesadas y sus expectativas	N-12	13	P35; T19	**Parcial**	SEVEN-G no tiene un registro de partes interesadas; lo cubre la tesis de C2.
4.3–4.4	Alcance y establecimiento del sistema de gestión	N-12	01 §5; 13; 90 §2	P32, P35	Directa	—
5.1–5.2	Liderazgo de la dirección y política de IA	N-12	13; 31; 60	P35, P43	Directa	—
5.3	Roles, responsabilidades y autoridades	N-06	01 §8; 30	P03, P38; T01	Directa	—
6.1.1–6.1.3	Riesgos y oportunidades; evaluación y tratamiento de riesgos de IA; declaración de aplicabilidad	N-10	13; 33	P12, P13, P74; T06	Directa	—
6.1.4	Evaluación de impacto de los sistemas de IA	N-10	32; 34 §3.10	P11, P47, P48; T07	Directa	—
6.2–6.3	Objetivos de IA y planificación de los cambios	N-09, N-12	13; 14; 40	P08, P35, P36; T11	Directa	—
7.1–7.3	Recursos, competencia y toma de conciencia	—	14; 31 §6; 50	P20, P45; T20	Directa	—
7.4–7.5	Comunicación e información documentada	N-02, N-07	03 §4; 21 §4; 60	P29; T01, T03, T17	Directa	—
8.1–8.4	Planificación y control operacional; evaluación de riesgos e impacto a intervalos planificados	N-04, N-10, N-11	20; 21; 52	P11, P12, P29, P65; T01, T03	Directa	—
9.1	Seguimiento, medición, análisis y evaluación	N-13	40; 41; 52	P25, P28; T12, T17	Directa	—

Ref.	Tema (resumen propio)	Núcleo	Dónde en SEVEN-G	Evidencia	Cobertura	Nota
9.2	Auditoría interna	—	38	P58–P60	Directa	—
9.3	Revisión por la dirección	N-12	01 §5 (C5); 60	P37; T15, T17	Directa	—
10.1–10.2	Mejora continua; no conformidad y acción correctiva	N-14	37; 01 §12	P50, P52; T08	Directa	—
Anexo A (A.2–A.10)	Controles de referencia por grupo (políticas, organización, recursos, impacto, ciclo de vida, datos, información a partes interesadas, uso, terceros)	N-01, N-10	34 §4.2	P74	**Parcial**	La declaración de aplicabilidad se hace control a control con P74 y debe cotejarse con el texto adquirido de la norma.
Certificación	Auditoría de certificación del sistema de gestión por una entidad acreditada	—	38 §12	—	**Requiere control externo**	SEVEN-G no certifica (D25); la certificación la emite una entidad acreditada según ISO/IEC 42006.

ISO/IEC 38507:2022 · Gobierno de la IA por el órgano de gobierno

Ref.	Tema (resumen propio)	Núcleo	Dónde en SEVEN-G	Evidencia	Cobertura	Nota
Por tema	Responsabilidad del órgano de gobierno sobre el uso de la IA y su rendición de cuentas	N-12	01 §5; 13; 30; 60; 61	P35, P39, P67; T17, T18	Directa	—
Por tema	Supervisión de las decisiones que se apoyan en la IA y de su grado de automatización	N-08	35 §5 (autonomía A0–A3); 21 (supervisión humana)	P17, P18	Directa	—
Por tema	Gobierno del uso de los datos por la IA	N-10	51; 34 §6	P47, P64	Directa	—

Ref.	Tema (resumen propio)	Núcleo	Dónde en SEVEN-G	Evidencia	Cobertura	Nota
Por tema	Riesgo, apetito y cumplimiento en el uso de la IA	N-10, N-12	13; 33; 34	P12, P35	Directa	—
Por tema	Cultura, valores y comportamiento esperados en el uso de la IA	—	31; 50; 23	P43, P45	**Parcial**	SEVEN-G regula el uso aceptable y la alfabetización; la cultura y los valores corporativos los define cada compañía.
Por tema	Valor y oportunidad estratégica de la IA para la organización	N-09, N-12, N-13	10; 12; 13; 40	P35; T14, T17	Directa	—

ISO/IEC 23894:2023 · Gestión del riesgo de la IA

Ref.	Tema (resumen propio)	Núcleo	Dónde en SEVEN-G	Evidencia	Cobertura	Nota
4	Principios de la gestión del riesgo aplicados a la IA	N-10	33 §1–§3	P12	Directa	—
5	Marco de referencia: liderazgo, integración, diseño, implementación, evaluación y mejora de la gestión del riesgo	N-06, N-12	13; 30; 33	P35, P38	Directa	—
6.2–6.3	Comunicación y consulta; alcance, contexto y criterios del riesgo	N-12	13 §5; 33 §4	P35; T06	Directa	—
6.4	Evaluación del riesgo: identificación, análisis y valoración	N-10	33 §4–§9 (escala 5 × 5 y 74 riesgos tipo)	P12; T06	Directa	—
6.5	Tratamiento del riesgo	N-10	33 §8; 35	P13, P18; T06	Directa	—
6.6–6.7	Seguimiento y revisión; registro e informe	N-11, N-13	33 §10–§11; 52; 60	P25, P65; T06, T17	Directa	—

ISO/IEC 42005:2025 · Evaluación del impacto de los sistemas de IA

Ref.	Tema (resumen propio)	Núcleo	Dónde en SEVEN-G	Evidencia	Cobertura	Nota
Por tema	Proceso de evaluación de impacto: cuándo se hace, alcance, responsables e integración con otros procesos	N-10	32; 20 (fase 3); 21 (G3.09, G4.13)	P11	Directa	—
Por tema	Información del sistema de IA, sus datos, su modelo y su entorno de despliegue	N-01	32; 51	P05, P15, P16, P64	Directa	—
Por tema	Partes interesadas e impactos reales y razonablemente previsibles sobre personas, colectivos y sociedad	N-10	34 §3.10; 50	P11, P48	Directa	—
Por tema	Usos sensibles o restringidos y umbrales que exigen una evaluación más profunda	N-03, N-10	01 §9.2; 32; 34 §3.4	P04, P11	**Parcial**	SEVEN-G usa los criterios Enterprise y la clasificación regulatoria como umbral; los usos restringidos propios los fija cada compañía en C2 (líneas rojas).
Por tema	Medidas para abordar los impactos, aprobación, registro, seguimiento y revisión de la evaluación	N-07, N-11	21; 52 (R6)	P11, P13, P29, P65; T07	Directa	—

NIST AI RMF 1.0

Ref.	Tema (resumen propio)	Núcleo	Dónde en SEVEN-G	Evidencia	Cobertura	Nota
GOVERN	Cultura y estructura de gobierno del riesgo de la IA	N-06, N-12	30; 31; 34 §5.4	P38, P73	Directa	Detalle por subcategoría en 34 §5.4 (72 subcategorías) y P73.
MAP	Contexto, categorización y riesgos de cada sistema	N-01, N-10	20; 32; 33	P04, P05, P11, P12	Directa	—

Ref.	Tema (resumen propio)	Núcleo	Dónde en SEVEN-G	Evidencia	Cobertura	Nota
MEASURE	Medición, pruebas y seguimiento de riesgos y fiabilidad	N-11, N-13	41; 52; 53	P22, P25, P53	Directa	—
MANAGE	Priorización, tratamiento, respuesta y comunicación de los riesgos	N-10, N-14	33; 37; 52	P13, P26, P50	Directa	—

Reglamento (UE) 2024/1689 (Reglamento Europeo de IA)

Ref.	Tema (resumen propio)	Núcleo	Dónde en SEVEN-G	Evidencia	Cobertura	Nota
Art. 4	Alfabetización en IA del personal	—	31 §6; 50	P45	Directa	—
Art. 5	Prácticas prohibidas	N-08, N-10	34 §3.4; 21 (G0.04, G3.08)	P02, P11	Directa	—
Art. 6 y anexos I y III	Clasificación como sistema de alto riesgo	N-10	32; 34 §3.6	P11; T05	Directa	—
Arts. 9, 10, 12, 14 y 15	Requisitos de los sistemas de alto riesgo: gestión de riesgos, datos, registros, supervisión humana, precisión, robustez y ciberseguridad	N-08, N-10	33; 51; 35; 34 §3.7	P12, P16, P17, P18, P22, P25	**Parcial**	Lo que SEVEN-G pide es necesario pero no suficiente para un proveedor de alto riesgo: debe completarse con las normas armonizadas aplicables.
Arts. 11 y 17 y anexo IV	Documentación técnica y sistema de gestión de la calidad del proveedor de alto riesgo	—	32 §6.3	—	**Requiere control externo**	SEVEN-G 0.x no incluye plantillas de documentación técnica ni de sistema de gestión de la calidad (D69).
Arts. 43, 47 y 48	Evaluación de la conformidad, declaración UE y marcado CE	—	34 §3.8	—	**Requiere control externo**	Procedimiento del proveedor con organismo notificado cuando proceda; SEVEN-G solo lo sitúa en la fase 5.

Ref.	Tema (resumen propio)	Núcleo	Dónde en SEVEN-G	Evidencia	Cobertura	Nota
Art. 13	Instrucciones de uso y transparencia hacia el responsable del despliegue	—	34 §3.7	P49	Directa	—
Art. 26	Obligaciones del responsable del despliegue	N-11	34 §3.9; 52	P17, P20, P24, P25	Directa	—
Art. 27	Evaluación de impacto en derechos fundamentales	N-10	34 §3.10	P48	Directa	—
Art. 49	Registro en la base de datos de la UE	—	34 §3.13	P11	**Parcial**	SEVEN-G recuerda la obligación y su evidencia; el registro lo hace la compañía en la base de datos.
Art. 50	Obligaciones de transparencia	N-08	34 §3.11; 21 (G4.05)	P17, P49	Directa	—
Arts. 51 a 55	Obligaciones de los proveedores de modelos de IA de uso general	—	34 §3.12	—	**No cubierto**	SEVEN-G cubre solo a quien integra un modelo de uso general, no a su proveedor.
Arts. 72 y 73	Vigilancia posterior a la comercialización e incidentes graves	N-11, N-14	34 §3.14–§3.15; 37; 52	P25, P26, P51; T08	Directa	—
Art. 99	Régimen sancionador	—	34 §3.16	—	**No cubierto**	Se cita a título informativo; no es una obligación que SEVEN-G gestione.

10

Procedimiento de mantenimiento del mapeo

10.1 Responsabilidades

Rol u órgano	Responsabilidad sobre el mapeo
Oficina de IA	Es la propietaria del documento 34 y de la herramienta T07. Mantiene la vigilancia normativa, prepara las propuestas de cambio y comunica los cambios aprobados.
Segunda línea (cumplimiento, asesoría jurídica, delegado de protección de datos, seguridad de la información)	Valida el contenido jurídico de cada cambio y su interpretación. Ningún cambio de fecha, artículo o criterio se publica sin su validación.
Comité de IA	Aprueba los cambios con impacto en casos de uso, *gates* o intensidad, y decide las reclasificaciones de la cartera.
Comisión delegada del consejo	Recibe trimestralmente el resumen de cambios regulatorios relevantes (C4).
Tercera línea	Verifica al menos una vez al año que el mapeo está actualizado y que los cambios se han aplicado a los casos de uso afectados.

10.2 Disparadores y periodicidad

Disparador	Ejemplos	Plazo de análisis
Publicación de una norma o modificación en el Diario Oficial de la UE o en el BOE	Nuevo reglamento modificativo; ley orgánica española; transposición de NIS2	10 días hábiles desde la publicación
Directrices, códigos de práctica, plantillas o actos de ejecución de la Comisión	Directrices finales sobre alto riesgo; plantilla de incidentes graves	20 días hábiles
Normas armonizadas o revisiones de normas técnicas	Normas de CEN-CENELEC JTC 21; revisión de ISO/IEC 42001; revisión del NIST AI RMF	30 días hábiles
Guías de autoridades nacionales o del CEPD; sentencias del TJUE	Guías AESIA; directrices del CEPD en versión final	20 días hábiles
Fecha de aplicación próxima	Seis meses antes de cada fecha del calendario de la sección 3.1	Revisión de los casos de uso afectados
Revisión ordinaria	Vigilancia mensual; revisión formal trimestral (C4); revisión completa anual (C5)	Según calendario

10.3 Pasos

Paso	Qué se hace	Responsable	Evidencia
1	Detectar el cambio y registrarlo con fuente oficial y fecha de consulta	Oficina de IA	Entrada en el registro de cambios del mapeo
2	Analizar el impacto: filas afectadas, preguntas de T07, criterios de *gate* (documento 21), plantillas y sistemas del inventario	Oficina de IA con segunda línea	Nota de impacto
3	Validar la interpretación jurídica	Segunda línea	Conformidad registrada
4	Aprobar el cambio si afecta a casos de uso, intensidad o *gates*	Comité de IA	P29 o acta del comité
5	Actualizar el documento 34 (nueva versión), T07 y, en su caso, las plantillas	Oficina de IA	Control de versiones
6	Reclasificar los sistemas afectados y abrir las acciones en los casos de uso (evento de cambio de clasificación en T01)	Responsables de riesgos de cada caso de uso	P11 actualizada; evento en T01
7	Comunicar a los equipos y, si es relevante, a la comisión delegada	Oficina de IA	Informe C4
8	Verificar la aplicación en la siguiente revisión anual	Tercera línea	Informe de auditoría (documento 38)

Un cambio regulatorio que convierte en incumplimiento una situación hasta entonces conforme no es por sí mismo una no conformidad; lo es no actuar en los plazos anteriores o dejar vencer una obligación aplicable (documento 37).

11

Anexo A · Otras jurisdicciones (orientativo)

Solo sirve para detectar posibles obligaciones fuera de la UE; no analiza requisitos y exige asesoramiento local.

Jurisdicción	Situación orientativa a fecha de consulta	Tratamiento en SEVEN-G
Reino Unido	La Data (Use and Access) Act 2025 (sección 80) sustituye el art. 22 del UK GDPR sobre decisiones automatizadas por los arts. 22A a 22D, plenamente en vigor desde el 5-02-2026. El resto del marco del Reino Unido no se mapea en este documento y debe verificarse con asesoramiento local.	Declararlo como restricción en P02 y consultar con asesoría local en la fase 3.
Estados Unidos	Este documento no mapea la regulación federal, sectorial ni estatal de Estados Unidos, que cambia con frecuencia: debe verificarse en las fuentes oficiales de cada jurisdicción con asesoramiento local. Como marco voluntario de referencia se usa el NIST AI RMF (sección 5).	Declararlo en P02; usar la sección 5 como referencia de buenas prácticas.
Instrumentos internacionales	Principios de IA de la OCDE (versión de 2024); Convenio Marco del Consejo de Europa sobre IA y derechos humanos, democracia y Estado de Derecho (abierto a la firma en Vilna el 5-09-2024; la Unión Europea lo ratificó el 15-05-2026).	Referencia para la política corporativa (documento 31).

12

Anexo B · Referencias sectoriales (orientativo)

No afirma requisitos sectoriales; señala interacciones que la segunda línea debe analizar en P02 y P11. Es solo orientativo: la responsabilidad de identificar la regulación sectorial aplicable, de la clasificación regulatoria y del cumplimiento es de la organización, con asesoramiento cualificado.

Sector	Puntos de contacto con el Reglamento de IA	Referencias sectoriales a revisar
Banca y pagos	Evaluación de solvencia y puntuación crediticia de personas físicas (anexo III, punto 5.b, salvo detección de fraude); integración de obligaciones en el gobierno interno (arts. 17.4 y 26.5); DORA (sección 7.1).	Ejercicio de mapeo de la EBA sobre el Reglamento de IA («AI Act: implications for the EU banking and payments sector», noviembre de 2025), sin necesidad inmediata de nuevas directrices; directrices de la EBA sobre concesión de préstamos; papel del Banco de España como autoridad (pendiente de la ley orgánica).
Seguros	Evaluación de riesgos y fijación de precios en seguros de vida y salud (anexo III, punto 5.c); DORA.	Dictamen de EIOPA sobre gobierno y gestión del riesgo de la IA (6-08-2025), dirigido a supervisores, que no crea nuevos requisitos y excluye los sistemas de alto riesgo y prohibidos; Solvencia II y Directiva de distribución de seguros.

Sector	Puntos de contacto con el Reglamento de IA	Referencias sectoriales a revisar
Sanidad	Productos sanitarios y de diagnóstico *in vitro* con IA como alto riesgo por el art. 6.1 y el anexo I (aplicación 2-08-2028); triaje de llamadas de emergencia y acceso a prestaciones públicas (anexo III, punto 5); categorías especiales de datos (RGPD art. 9).	Reglamentos (UE) 2017/745 y 2017/746; Reglamento (UE) 2025/327, del Espacio Europeo de Datos de Salud, aplicable con carácter general desde el 26-03-2027 y con disposiciones desde el 26-03-2029 y el 26-03-2031 (art. 105); normativa sanitaria nacional.
Pagos: identificación de terceros (PSD2)	Un agente que actúa por el cliente sobre sus cuentas es, en la práctica, un tercero ante la entidad.	Directiva (UE) 2015/2366 y Reglamento Delegado (UE) 2018/389: el tercero proveedor puede identificarse ante la entidad que gestiona la cuenta (art. 30) y la entidad debe asegurar que puede identificarse también en el mecanismo de reserva (art. 33); esta lectura se limita a esos artículos y no afirma que la norma prohíba o permita por sí misma el acceso por pantalla.
Pagos: quién autentica al cliente (opinión de la EBA)	Si un agente inicia un pago por el cliente, alguien tiene que aplicar la autenticación reforzada y responder de ella.	Opinión de la EBA sobre la aplicación de las normas técnicas de autenticación reforzada (EBA-Op-2018-04, 13 de junio de 2018; eba.europa.eu): la autenticación reforzada la aplica, y sus exenciones las decide, el proveedor de servicios de pago que emite las credenciales del cliente; el tercero proveedor se identifica ante la entidad y no decide las exenciones; la entidad puede encargar por contrato a otro proveedor que haga la autenticación en su nombre, y entre ellos reparten la responsabilidad; la autenticación se exige en cada inicio de pago, también dentro de una sesión ya autenticada, salvo exención; un tercero puede consultar la cuenta sin el cliente presente cuatro veces al día como máximo. La opinión es de 2018, se dirige a las autoridades competentes y solo trata los terceros proveedores regulados: **no menciona los agentes de IA**. Se cita como orientación para diseñar el canal, no como norma sobre agentes.
Identidad digital (eIDAS 2)	Una credencial verificable podría servir de base para identificar a un agente y a quien responde de él.	Reglamento (UE) 2024/1183: crea el marco de las carteras europeas de identidad digital y de las declaraciones electrónicas de atributos; **no regula la identidad de agentes de IA** ni la exige.
Servicios de pago: propuesta (borrador)	Posible evolución de las reglas de pago, con efecto sobre terceros y agentes.	Propuesta de Reglamento de servicios de pago, COM(2023) 367, y propuesta de directiva paralela: propuesta en tramitación (borrador), no norma vigente; su estado actual no se ha comprobado y no fundamenta ningún control.

13

Anexo C · Fuentes consultadas y estado de verificación

Fecha de consulta: 16-09-2026, salvo las fuentes de la sección 5.3, la correspondencia de la sección 4.3 y la ficha de ISO/IEC 42001 , consultadas el 25-09-2026.

Tema	Fuente	Estado
Ómnibus: tramitación, entrada en vigor (27-07-2026), fechas de alto riesgo, art. 50.2 y nuevas prohibiciones	Comisión Europea (digital-strategy.ec.europa.eu; AI Act Service Desk); Parlamento Europeo, procedimiento 2025/0359(COD)	Verificado (oficial)
Texto del Reglamento (UE) 2026/1744 y detalle de los arts. 3.14, 4, 4 bis, 5, 10, 49, 72, 111 y anexos I y VIII	EUR-Lex (texto oficial cotejado con el navegador)	Verificado (oficial)
Directrices y códigos de la Comisión	Comisión Europea	Verificado (oficial); finales de alto riesgo e incidentes graves pendientes
ISO/IEC 42001, 42005 y 42006; NIST AI RMF y AI 600-1; CEPD	iso.org; nist.gov; edpb.europa.eu	Verificado (oficial)
NIST CSF 2.0 (NIST CSWP 29, versión final de 26-02-2024)	csrc.nist.gov; nist.gov/cyberframework (traducción oficial al español)	Verificado (oficial)
Cyber AI Profile (NIST IR 8596, borrador preliminar inicial de 16-12-2025)	csrc.nist.gov; nccoe.nist.gov (el proyecto está revisando comentarios)	Verificado (oficial); **Borrador**
Correspondencia AI RMF ↔ ISO/IEC 42001 (aportada por Microsoft sobre el FDIS de 2023)	airc.nist.gov	Verificado (oficial) en cuanto a su existencia y autoría; orientativa, no la firma NIST
Parte del ómnibus que modifica el RGPD	EUR-Lex, COM(2025) 837 final; Parlamento Europeo, procedimiento 2025/0360(COD)	Verificado (oficial): en tramitación, no adoptada
RD 729/2023 , RD 817/2023 , guías AESIA , proyecto de ley orgánica	boe.es; aesia.digital.gob.es; La Moncloa; congreso.es	Verificado (oficial); estado posterior al 16-09-2026 pendiente

Tema	Fuente	Estado
Transposición de NIS2 en España; Reino Unido; Espacio Europeo de Datos de Salud; Convenio Marco del Consejo de Europa	dsn.gob.es, lamoncloa.gob.es y Comisión Europea (IP/26/1499); legislation.gov.uk; EUR-Lex; coe.int	Verificado (oficial)
Ciberresiliencia; EBA; EIOPA	Comisión Europea; eba.europa.eu; eiopa.europa.eu	Verificado (oficial)
PSD2, Reglamento Delegado (UE) 2018/389, eIDAS 2 y propuesta de reglamento de servicios de pago (identificación de terceros y de agentes, 12)	EUR-Lex (textos oficiales: arts. 30 y 33 del Reglamento Delegado; art. 1 y art. 3 de eIDAS 2; COM(2023) 367)	Verificado (oficial); la propuesta de servicios de pago es **Borrador** y su estado actual no se ha comprobado
Opinión de la EBA sobre la aplicación de las normas técnicas de autenticación reforzada (EBA-Op-2018-04, 12)	eba.europa.eu (texto oficial, leído entero el 19-11-2026 en el PDF descargado por el autor)	Verificado (oficial); es una opinión dirigida a las autoridades competentes, no una norma
Protocolos de agente: Web Bot Auth (IETF) y Personal Agent Protocol	datatracker.ietf.org; sierra.ai (publicación del 6-10-2026 del impulsor del protocolo)	Verificado (oficial) en cuanto a su existencia y propósito; ambos son **Borrador** y no fundamentan ningún control
Propuestas del sector financiero europeo sobre agentes de IA: «Know Your Agent», permisos revocables y responsabilidad ligada al control	Tribuna de Carlos Torres Vila (presidente de BBVA), «Los agentes personales de IA no deberían tener que "hacerse pasar" por nosotros», Expansión (sección Financial Times), 13-11-2026	Leída entera el 15-11-2026; **opinión y propuestas de su autor, no norma**
Consultoría y estudio académico sobre el cliente agéntico	Bain & Company, «When Your Customer Sends an Agent» (10-11-2026); Park et al., arXiv:2411.10109	Verificado (el estudio académico, solo el resumen); no fundamentan ninguna regla

14

Herramientas y plantillas asociadas

Código	Uso en este documento
T07 · Clasificador regulatorio	Herramienta principal: determinaciones de la sección 2, preguntas de los arts. 5, 6 y 50, evaluaciones requeridas y fechas de la sección 3.1. Se actualiza con el procedimiento de la sección 10.

Código	Uso en este documento
T02 · T03 · T06 · T08 · T09 · T10	Inventario y registro UE · verificación en *gates* · riesgos · incidentes y notificaciones · cadena de valor y terceros · ciberseguridad y supervisión humana.
T17 · T20 · T21	Reporte al consejo, formación y uso corporativo.
P11 · Clasificación regulatoria y evaluaciones de impacto	Evidencia principal de la fase 3.
P47 · Evaluación de impacto en protección de datos	Evidencia de RGPD arts. 35 y 36 (sección 6.1).
P48 · Evaluación de impacto en derechos fundamentales	Evidencia del art. 27 y de su notificación (sección 3.10).
P49 · Avisos de transparencia e instrucciones de uso	Evidencia del art. 50 (sección 3.11).
P72 · Perfil de seguridad de IA (CSF 2.0 / Cyber AI Profile)	Perfil actual y objetivo de las subcategorías de la sección 5.5 (secciones 5.3 y 5.5).
P73 · Perfil de gobierno de IA (NIST AI RMF)	Perfil actual y objetivo de las 72 subcategorías de la sección 5.4.
P74 · Declaración de aplicabilidad de ISO/IEC 42001	Controles del anexo A aplicables, justificación, cobertura y evidencia (secciones 4.1, cláusula 6.1.3, y 4.2).
P02, P05 · P12–P18 · P21–P27 · P29	Clasificación provisional · requisitos de diseño · conformidad, operación e incidentes · decisiones y cambios del mapeo.

15

Documentos relacionados

Documento	Relación
01 · Metodología fundacional	Sección 13, que este documento desarrolla.
03 · Herramientas	Catálogo y taxonomía regulatoria.
21 · Criterios de *gate*	Verificación de evidencias regulatorias.
30 · Modelo de gobierno	Segunda línea, escalado y notificaciones.
31 · Política corporativa	Alfabetización y uso corporativo.

Documento	Relación
32 · Inventario y clasificación	Procedimiento de clasificación.
33 · Riesgos de IA	Impacto regulatorio y riesgos tipo.
35 · Seguridad de IA y agentes	Ciberseguridad y ciberresiliencia.
36 · Terceros	Cadena de valor y DORA.
37 · No conformidades e incidentes	Incidentes graves.
38 · Auditoría de IA	Verificación anual del mapeo.
53 · Construcción con IA	Evidencias de desarrollo.

16

Control de versiones

Versión	Fecha	Cambios
0.1	16-09-2026	Primera versión. Mapea el Reglamento Europeo de IA con las modificaciones del Reglamento (UE) 2026/1744 (calendario verificado a 16-09-2026), ISO/IEC 42001:2023, NIST AI RMF 1.0 y NIST AI 600-1, RGPD y guías del CEPD, DORA, NIS2 y normativa española; añade matriz resumen, procedimiento de mantenimiento y anexos orientativos de otras jurisdicciones y sectores. Aviso legal y responsabilidad del usuario sobre el cumplimiento regulatorio.
0.2	25-09-2026	Añade la sección 5.3, NIST CSF 2.0 y Cyber AI Profile: funciones del CSF aplicadas a los sistemas de IA, áreas Secure, Defend y Thwart del perfil (en borrador) y advertencia de que los *tiers* no son niveles de madurez por subcategoría; el estado «Borrador» en la sección 1.4; la columna del CSF en la matriz resumen; la correspondencia AI RMF ↔ ISO/IEC 42001 del AIRC en la sección 4.3; las fuentes nuevas en la sección 13; y las secciones 5.4 (las 72 subcategorías del AI RMF) y 5.5 (las 48 subcategorías del CSF 2.0 con prioridad alta en el Cyber AI Profile, selección provisional), con su cobertura en SEVEN-G y la pregunta del documento 11 que da su nivel. Corrige el estado de ISO/IEC 42001: publicada (etapa 60.60), sin revisión en curso. Enlaza las plantillas P72 (perfil de seguridad de IA), P73 (perfil de gobierno de IA) y P74 (declaración de aplicabilidad de ISO/IEC 42001). Sustituye las afirmaciones que no se apoyaban en una fuente oficial por su fuente oficial (Reglamento (UE) 2026/1744 en EUR-Lex, NIS2 en España, Reino Unido, Espacio Europeo de Datos de Salud, Convenio Marco del Consejo de Europa y propuesta de modificación del RGPD) y retira el estado de verificación que admitía análisis de terceros.
0.3	25-09-2026	El área Defend del Cyber AI Profile (en borrador) pasa a tener cobertura: sección 9.3 del documento 35, controles SEG-21 a SEG-25 y riesgo tipo RT-SEG-08.

Versión	Fecha	Cambios
0.4	01-10-2026	Añade la sección 9.1, crosswalk de cobertura con ISO/IEC 42001, ISO/IEC 38507, ISO/IEC 23894, ISO/IEC 42005, el NIST AI RMF y el Reglamento Europeo de IA: por cada requisito, dónde lo cubre SEVEN-G, con qué regla del núcleo, con qué evidencia y con qué cobertura (directa, parcial, requiere control externo o no cubierto). Las tablas se generan desde `crosswalk.json`.
0.5	19-10-2026	Área Secure con la pasarela corporativa de IA (SEG-26) y el banco de pruebas corporativo de agentes (SEG-27); 72 riesgos tipo en el crosswalk (D159).
0.6	16-11-2026	Precisión en la sección 3.11 (el art. 50 no obliga a un agente a identificarse), tres filas en el anexo B (identificación de terceros en PSD2, eIDAS 2 y la propuesta de servicios de pago, en borrador) y las fuentes nuevas en el anexo C (D185).
0.7	19-11-2026	Anexo B: fila sobre quién aplica la autenticación reforzada del cliente según la opinión de la EBA de 2018 (EBA-Op-2018-04), leída entera; fuente en el anexo C (D194).

Fuentes externas citadas

Enlaces a la fuente oficial o primaria, comprobados antes de publicar. Verifique siempre la versión vigente en la fecha de uso.

Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior (PSD2) · https://eur-lex.europa.eu/eli/dir/2015/2366/oj/spa · Parlamento Europeo y Consejo de la UE · 25-11-2015

Directiva (UE) 2016/97 del Parlamento Europeo y del Consejo, de 20 de enero de 2016, sobre la distribución de seguros (versión refundida) · https://eur-lex.europa.eu/eli/dir/2016/97/oj/spa · Parlamento Europeo y Consejo de la UE · 20-01-2016

Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (Directiva SRI 2 / NIS2) · https://eur-lex.europa.eu/eli/dir/2022/2555/oj/spa · Parlamento Europeo y Consejo de la UE · 14-12-2022

Directiva 2009/138/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, sobre el seguro de vida, el acceso a la actividad de seguro y de reaseguro y su ejercicio (Solvencia II) (versión refundida) · https://eur-lex.europa.eu/eli/dir/2009/138/oj/spa · Parlamento Europeo y Consejo de la UE · 25-11-2009

Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifican los Reglamentos (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725, (UE) 2023/2854 y las Directivas 2002/58/CE, (UE) 2022/2555 y (UE) 2022/2557 en lo que respecta a la simplificación del marco legislativo digital y se derogan los Reglamentos (UE) 2018/1807, (UE) 2019/1150, (UE)

2022/868 y la Directiva (UE) 2019/1024 (Ómnibus Digital) · COM(2025) 837 final · procedimiento 2025/0360(COD) · https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52025PC0837 · Comisión Europea (propuesta); Parlamento Europeo y Consejo de la UE (tramitación) · 19-11-2025

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/spa · Parlamento Europeo y Consejo de la UE · 27-04-2016

Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios · https://eur-lex.europa.eu/eli/reg/2017/745/oj/spa · Parlamento Europeo y Consejo de la UE · 05-04-2017

Reglamento (UE) 2017/746 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios para diagnóstico in vitro · https://eur-lex.europa.eu/eli/reg/2017/746/oj/spa · Parlamento Europeo y Consejo de la UE · 05-04-2017

Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre la resiliencia operativa digital del sector financiero (DORA) · https://eur-lex.europa.eu/eli/reg/2022/2554/oj/spa · Parlamento Europeo y Consejo de la UE · 14-12-2022

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 y la Directiva 73/361/CEE · https://eur-lex.europa.eu/eli/reg/2023/1230/oj/spa · Parlamento Europeo y Consejo de la UE · 14-06-2023

Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital (eIDAS 2) · https://eur-lex.europa.eu/eli/reg/2024/1183/oj/spa · Parlamento Europeo y Consejo de la UE · 11-04-2024

Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial) · https://eur-lex.europa.eu/eli/reg/2024/1689/oj/spa · Parlamento Europeo y Consejo de la UE · 13-06-2024

Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales (Reglamento de Ciberresiliencia) · https://eur-lex.europa.eu/eli/reg/2024/2847/oj/spa · Parlamento Europeo y Consejo de la UE · 23-10-2024

Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo, de 11 de febrero de 2025, relativo al Espacio Europeo de Datos de Salud, y por el que se modifican la Directiva 2011/24/UE y el Reglamento (UE) 2024/2847 · https://eur-lex.europa.eu/eli/reg/2025/327/oj/spa · Parlamento Europeo y Consejo de la UE · 11-02-2025

Reglamento (UE) 2026/1744 del Parlamento Europeo y del Consejo, de 8 de julio de 2026, por el que se modifican los Reglamentos (UE) 2024/1689, (UE) 2018/1139 y (UE) 2023/1230 en lo que respecta a la simplificación de la aplicación de normas armonizadas en materia de inteligencia artificial (Ómnibus digital sobre IA) · https://eur-lex.europa.eu/eli/reg/2026/1744/oj/spa · Parlamento Europeo y Consejo de la UE · 08-07-2026

Reglamento Delegado (UE) 2018/389 de la Comisión, de 27 de noviembre de 2017, por el que se completa la Directiva (UE) 2015/2366 con normas técnicas de regulación para la autenticación reforzada de clientes y para unos estándares abiertos de comunicación comunes y seguros · https://eur-lex.europa.eu/eli/reg_del/2018/389/oj/spa · Comisión Europea · 27-11-2017

Convenio Marco del Consejo de Europa sobre Inteligencia Artificial y Derechos Humanos, Democracia y Estado de Derecho (STCE n.º 225), Vilna, 5 de septiembre de 2024 · https://eur-lex.europa.eu/eli/agree_internation/2026/1081/oj/spa · Consejo de Europa · 05-09-2024

Data (Use and Access) Act 2025 (c. 18) del Reino Unido, de 19 de junio de 2025; sección 80 (decisiones automatizadas, nuevos arts. 22A a 22D del UK GDPR) · https://www.legislation.gov.uk/ukpga/2025/18/contents · Parlamento del Reino Unido · 19-06-2025

Acuerdo de 28 de enero de 2026, del Pleno del Consejo General del Poder Judicial, por el que se aprueba la Instrucción 2/2026, sobre la utilización de sistemas de inteligencia artificial en el ejercicio de la actividad jurisdiccional · https://www.boe.es/eli/es/a/2026/01/28/(1) · Consejo General del Poder Judicial (Pleno) · 28-01-2026

Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad (aprobado en primera vuelta por el Consejo de Ministros el 14 de enero de 2025) · https://www.dsn.gob.es/es/actualidad/sala-de-prensa/anteproyecto-ley-coordinacion-gobernanza-ciberseguridad · Gobierno de España (Consejo de Ministros; Departamento de Seguridad Nacional) · 14-01-2025

Ley 2/2025, de 2 de abril, para el desarrollo e impulso de la inteligencia artificial en Galicia · https://www.boe.es/eli/es-ga/l/2025/04/02/2 · Comunidad Autónoma de Galicia (Parlamento de Galicia) · 02-04-2025

Proyecto de Ley Orgánica para el buen uso y la gobernanza de la inteligencia artificial (expediente 121/000096) · https://www.congreso.es/es/proyectos-de-ley?p_p_id=iniciativas&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&_iniciativas_mode=mostrarDetalle&_iniciativas_legislatura=XV&_iniciativas_id=121%2F000096 · Gobierno de España (Consejo de Ministros); Congreso de los Diputados (tramitación) · 26-05-2026

Real Decreto 729/2023, de 22 de agosto, por el que se aprueba el Estatuto de la Agencia Española de Supervisión de Inteligencia Artificial · https://www.boe.es/eli/es/rd/2023/08/22/729/con · Gobierno de España (Ministerio de Hacienda y Función Pública) · 22-08-2023

Real Decreto 817/2023, de 8 de noviembre, que establece un entorno controlado de pruebas para el ensayo del cumplimiento de la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial · https://www.boe.es/buscar/act.php?id=BOE-A-2023-22767 · Gobierno de España (Ministerio de Asuntos Económicos y Transformación Digital) · 08-11-2023

Sentencia del Tribunal de Justicia (Sala Primera) de 27 de febrero de 2025, CK contra Magistrat der Stadt Wien (Dun & Bradstreet Austria), asunto C-203/22, ECLI:EU:C:2025:117 · https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:62022CJ0203 · Tribunal de Justicia de la Unión Europea · 27-02-2025

Sentencia del Tribunal de Justicia (Sala Primera) de 7 de diciembre de 2023, OQ contra Land Hessen (SCHUFA Holding — Scoring), asunto C-634/21, ECLI:EU:C:2023:957 · https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:62021CJ0634 · Tribunal de Justicia de la Unión Europea · 07-12-2023

Agencia Española de Protección de Datos (AEPD) · https://www.aepd.es/ · Agencia Española de Protección de Datos

Agencia Española de Supervisión de Inteligencia Artificial (AESIA) · https://aesia.digital.gob.es/es · Agencia Española de Supervisión de Inteligencia Artificial

Banco de España · https://www.bde.es/wbe/es/ · Banco de España

Comité Europeo de Protección de Datos (CEPD) · https://www.edpb.europa.eu/edpb_es · Comité Europeo de Protección de Datos (organismo de la UE creado por el art. 68 del RGPD)

Oficina Europea de IA (Comisión Europea) · https://digital-strategy.ec.europa.eu/es/policies/ai-office · Comisión Europea (DG CONNECT)

Código de buenas prácticas de IA de uso general · https://digital-strategy.ec.europa.eu/es/policies/contents-code-gpai · Comisión Europea (Oficina Europea de IA), elaborado por expertos independientes · 10-07-2025

Código de buenas prácticas sobre transparencia de los contenidos generados por IA (marcado y etiquetado) · https://digital-strategy.ec.europa.eu/es/policies/code-practice-ai-generated-content · Comisión Europea (Oficina Europea de IA), elaborado por expertos independientes · 10-06-2026

Correspondencia del NIST AI RMF con ISO/IEC 42001 (NIST AI Risk Management Framework to ISO-IEC-42001 Crosswalk), publicada en el centro de recursos del AI RMF (AIRC) · https://airc.nist.gov/airmf-resources/crosswalks/ · Microsoft (aportada por un tercero y alojada por NIST en el AIRC) · 23-05-2023

Declaración 3/2024 sobre el papel de las autoridades de protección de datos en el marco de la Ley de Inteligencia Artificial · https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-32024-data-protection-authorities-role-artificial_es · Comité Europeo de Protección de Datos · 16-07-2024

Dictamen 28/2024 sobre determinados aspectos de la protección de datos relacionados con el tratamiento de datos personales en el contexto de los modelos de IA · https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_es · Comité Europeo de Protección de Datos · 17-12-2024

Dictamen de EIOPA sobre gobierno y gestión del riesgo de la inteligencia artificial (EIOPA-BoS-25-360), de 6 de agosto de 2025 · https://www.eiopa.europa.eu/publications/opinion-artificial-intelligence-governance-and-risk-management_en · Autoridad Europea de Seguros y Pensiones de Jubilación (EIOPA) · 06-08-2025

Directrices 01/2025 sobre seudonimización (versión 1.0 para consulta pública) · https://www.edpb.europa.eu/public-consultations/guidelines-012025-on-pseudonymisation_en · Comité Europeo de Protección de Datos · 16-01-2025

Directrices 02/2026 sobre anonimización (versión 1.0 para consulta pública) · https://www.edpb.europa.eu/public-consultations/guidelines-022026-on-anonymisation_en · Comité Europeo de Protección de Datos · 07-07-2026

Directrices 03/2026 sobre extracción web (web scraping) en el contexto de la IA generativa (versión 1.0 para consulta pública) · https://www.edpb.europa.eu/public-consultations/guidelines-032026-on-web-scraping-in-the-context-of-generative-ai_en · Comité Europeo de Protección de Datos · 07-07-2026

Directrices 4/2019 relativas al artículo 25 Protección de datos desde el diseño y por defecto (versión 2.0) · https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_es · Comité Europeo de Protección de Datos · 20-10-2020

Directrices de la Comisión sobre la definición de sistema de inteligencia artificial establecida por el Reglamento (UE) 2024/1689 (Reglamento de IA) · https://digital-strategy.ec.europa.eu/es/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application · Comisión Europea · 06-02-2025

Directrices de la Comisión sobre prácticas de inteligencia artificial prohibidas establecidas por el Reglamento (UE) 2024/1689 (Reglamento de IA) · https://digital-strategy.ec.europa.eu/es/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act · Comisión Europea · 04-02-2025

Directrices de la EBA sobre concesión y seguimiento de préstamos (EBA/GL/2020/06), de 29 de mayo de 2020 · https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/credit-risk/guidelines-loan-origination-and-monitoring · Autoridad Bancaria Europea (EBA) · 29-05-2020

Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679 (WP251 rev.01), del Grupo de Trabajo del Artículo 29, asumidas por el CEPD · https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/automated-decision-making-and-profiling_es · Grupo de Trabajo del Artículo 29; asumidas por el Comité Europeo de Protección de Datos (25-05-2018) · 06-02-2018

Directrices sobre el alcance de las obligaciones de los proveedores de modelos de IA de uso general en virtud del Reglamento de IA · https://digital-strategy.ec.europa.eu/es/library/guidelines-scope-obligations-providers-general-purpose-ai-models-under-ai-act · Comisión Europea · 18-07-2025

Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento 2016/679 (WP248 rev.01), del Grupo de Trabajo del Artículo 29, asumidas por el CEPD · https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/data-protection-impact-assessments-high-risk-processing_es · Grupo de Trabajo del Artículo 29; asumidas por el Comité Europeo de Protección de Datos (25-05-2018) · 04-10-2017

Directrices sobre las obligaciones de transparencia de los proveedores y responsables del despliegue de determinados sistemas de IA (art. 50 del Reglamento de IA) · https://digital-strategy.ec.europa.eu/es/library/guidelines-transparency-obligations-providers-and-deployers-ai-systems · Comisión Europea · 20-07-2026

Guías de apoyo al cumplimiento del Reglamento de IA (16 guías: 2 introductorias, 13 técnicas y manual de listas de verificación con compendio) · https://aesia.digital.gob.es/es/guias · Agencia Española de Supervisión de Inteligencia Artificial (AESIA) · 16-12-2025

Guías de la AEPD sobre tratamientos que incorporan IA: «Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción» (febrero de 2020) y «Requisitos para Auditorías de Tratamientos que incluyan IA» (enero de 2021) · página «Innovación y Tecnología» que reúne ambas · https://www.aepd.es/areas-de-actuacion/innovacion-y-tecnologia · Agencia Española de Protección de Datos

Marco de gestión de riesgos de IA: perfil de inteligencia artificial generativa (NIST AI 600-1) · https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-generative-artificial-intelligence · National Institute of Standards and Technology (NIST) · 26-07-2024

Nota explicativa y plantilla para el resumen público del contenido de entrenamiento de los modelos de IA de uso general · https://digital-strategy.ec.europa.eu/es/library/explanatory-notice-and-template-public-summary-training-content-general-purpose-ai-models · Comisión Europea (Oficina Europea de IA) · 24-07-2025

Orientaciones de la Comisión, con plantilla, sobre el plan de vigilancia poscomercialización (art. 72.3 del Reglamento de IA, en la redacción del Reglamento (UE) 2026/1744) · https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:02024R1689-20260727 · Comisión Europea

Perfil del marco de ciberseguridad para la inteligencia artificial (Cyber AI Profile): perfil comunitario del NIST, NIST IR 8596 (borrador preliminar inicial) · https://csrc.nist.gov/pubs/ir/8596/iprd · National Institute of Standards and Technology (NIST), NCCoE · 16-12-2025

Proyecto de directrices de la Comisión sobre la clasificación de los sistemas de IA de alto riesgo · https://digital-strategy.ec.europa.eu/es/library/draft-commission-guidelines-classification-high-risk-ai-systems · Comisión Europea · 19-05-2026

Proyecto de orientaciones y plantilla de notificación de incidentes graves de IA (art. 73 del Reglamento de IA) · https://digital-strategy.ec.europa.eu/es/consultations/ai-act-commission-issues-draft-guidance-and-reporting-template-serious-ai-incidents-and-seeks · Comisión Europea · 26-09-2025

CEN-CLC/JTC 21 «Artificial Intelligence»: normas europeas (armonizadas) en apoyo del Reglamento de IA · https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/artificial-intelligence/ · CEN y CENELEC (Comité Técnico Conjunto 21), a petición de normalización de la Comisión Europea

ISO/IEC 23894:2023 Tecnología de la información — Inteligencia artificial — Orientación sobre la gestión del riesgo · https://www.iso.org/standard/77304.html · ISO/IEC (JTC 1/SC 42) · 06-02-2023

ISO/IEC 38507:2022 Tecnología de la información — Gobierno de las TI — Implicaciones para el gobierno del uso de la inteligencia artificial por las organizaciones · https://www.iso.org/standard/56641.html · ISO/IEC (JTC 1/SC 40) · 08-04-2022

ISO/IEC 42001:2023 Tecnología de la información — Inteligencia artificial — Sistema de gestión · https://www.iso.org/standard/42001 · ISO/IEC (JTC 1/SC 42) · 18-12-2023

ISO/IEC 42005:2025 Tecnología de la información — Inteligencia artificial (IA) — Evaluación de impacto de sistemas de IA · https://www.iso.org/standard/42005 · ISO/IEC (JTC 1/SC 42) · 28-05-2025

ISO/IEC 42006:2025 Tecnología de la información — Inteligencia artificial — Requisitos para los organismos que realizan auditoría y certificación de sistemas de gestión de IA · https://www.iso.org/standard/42006 · ISO/IEC (JTC 1/SC 42) · 07-07-2025

Marco de ciberseguridad del NIST, versión 2.0 (The NIST Cybersecurity Framework (CSF) 2.0), NIST CSWP 29 · https://doi.org/10.6028/NIST.CSWP.29.spa · National Institute of Standards and Technology (NIST), Departamento de Comercio de EE. UU. · 26-02-2024

Marco de gestión de riesgos de inteligencia artificial del NIST (AI RMF 1.0), NIST AI 100-1 · https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-ai-rmf-10 · National Institute of Standards and Technology (NIST), Departamento de Comercio de EE. UU. · 26-01-2023

Recomendación del Consejo de la OCDE sobre Inteligencia Artificial (OECD/LEGAL/0449), Principios de IA de la OCDE, adoptada el 22 de mayo de 2019 y modificada el 3 de mayo de 2024 · https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 · Organización para la Cooperación y el Desarrollo Económicos (OCDE) · 03-05-2024