

Inteligencia artificial

Ámbito 1 · EPSO/AD/430/26 · grado AD 8

240

aprobados buscados

AD 8

grado de entrada

30 / 40 min

examen del ámbito

13 oct 2026

cierre de solicitudes

eu-now.com

Dossier de preparación · 15 bloques de estudio con sus fuentes oficiales

Elaborado sobre la convocatoria DO C/2026/4668 y los textos oficiales que cubren su Anexo II

[EU-now.com](https://eu-now.com)

1 · La oposición de un vistazo

EPSO/AD/430/26 es una oposición general por titulación y pruebas para **administradores de grado AD 8** de las instituciones, órganos y organismos de la Unión. Dos ámbitos, **solo se puede elegir uno**: inteligencia artificial (240 aprobados buscados) y ciberseguridad (254). Tú vas a inteligencia artificial: 240 plazas en la lista de reserva.



Lo que decide todo: los tres tests de razonamiento y la redacción EUFTE son puertas de sí o no. **Solo la nota del MCQ del ámbito ordena a los candidatos**, y solo a los mejores se les corrige la EUFTE y se les comprueba la titulación. Dos tercios del tiempo de estudio, al ámbito.



Las cinco fases. Solo la puntuación del MCQ del ámbito ordena a los candidatos; el resto son puertas de sí o no.

2 · Las cinco pruebas

Prueba	Lengua	Preguntas	Duración	Puntos	Corte
Razonamiento verbal	1	20	35 min	0-20	10/20
Razonamiento numérico	1	10	20 min	0-10	10/20 junto con el abstracto
Razonamiento abstracto	1	10	10 min	0-10	10/20 junto con el numérico
MCQ del ámbito	2	30	40 min	0-30	15/30 y estar entre los mejores
EUFTE	2	—	40 min	0-10	5/10

Lengua 1 es cualquiera de las 24 oficiales. **Lengua 2** es la del MCQ del ámbito y la EUFTE. Hace falta C1 en una y B2 en la otra, y se eligen en el formulario. Las pruebas son a distancia con vigilancia remota, y el orden de convocatoria puede no ser el de la convocatoria.

La EUFTE no es un examen de idioma ni de conocimientos: EPSO publica documentación sobre asuntos de la Unión antes del examen, la misma que se entrega durante la prueba, y se responde a una consigna basada en ella. Se corrige con criterios publicados.

La plataforma del examen

Las pruebas se hacen en TAO, la plataforma que EPSO usa en todos sus exámenes. Conviene llegar sabiendo dónde está cada cosa: se pierde menos tiempo y no hay sorpresas el día de la prueba.

EU Careers - Sample Test / Part I / Verbal Reasoning
Pregunta 47a

Clock

All cells in the body have a specific structure and perform a specialised function, apart from stem cells. Stem cells have a number of remarkable properties. Unlike most specialised cells they are capable of replicating themselves many times. They can also develop into different types of specialised cells, such as muscle cells or red blood cells. These properties, in theory, mean that stem cells could repair the body, by multiplying and then replacing badly damaged tissue. It is believed that, in time, stem cell research could revolutionise medicine, as stem cells could be used to repair tissues or even to grow replacement organs.

Which of the following statements is correct?

☐ A. The only difference between stem cells and other cells is that stem cells do not perform a specialised function.

☐ B. A muscle cell that originated from a stem cell may transform back into a stem cell.

☐ C. Stem cells are the only cells that have the ability to repair themselves.

☐ D. Stem cells could repair damaged tissues by multiplying and then replacing damaged cells.

1. Elimination tool
2. Calculator
3. Scratchpad

Answered Answered and bookmarked Bookmarked

Back 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 OVERVIEW (16) Next

Bookmark tool

Pantalla de pregunta: navegador de preguntas abajo, marcador, reloj y herramientas arriba.

Verbal Reasoning

Test Configuration

Set

1013x2
2026

AC ± % ÷

Descartar opciones: tacha lo que ya has eliminado.

Resaltador y lector de líneas para enunciados largos.

Calculadora y bloc de notas donde la prueba los permite.

Capturas de la plataforma TAO utilizada en las pruebas de EPSO.

La lista de reserva se publica en orden alfabético, no por nota; los empates en la última plaza entran todos; y figurar en ella no garantiza contratación.

Fuentes: convocatoria DO C/2026/4668, secciones 1, 4.2, 4.3.1, 4.3.2 (tablas 3 a 5), 4.3.3 y 4.3.4.

3 · Cómo son las 30 preguntas

La convocatoria no publica temario ni bibliografía. El contrato es el **Anexo II, «funciones típicas»**: de ahí sale todo lo preguntable, y por eso este dossier lo desglosa entero. Son 30 preguntas en 40 minutos, en lengua 2: **80 segundos por pregunta**. No hay tiempo de deducir desde cero, se contesta con lo que se reconoce.

Enunciado con un caso de trabajo

Una autoridad nacional detecta un incidente significativo en una entidad esencial...

- ☐ A · Notificar en 72 horas al CSIRT
- ☒ B · Alerta temprana en 24 horas al CSIRT
- ☐ C · Informe final en un mes a la Comisión
- ☐ D · Notificar al Grupo de Cooperación

Lo que decide la respuesta

- 1** QUIÉN es competente
CSIRT, autoridad, Comisión...
- 2** QUÉ obligación exacta
alerta, notificación, informe
- 3** EL NÚMERO
24 h · 72 h · un mes

Los distractores atacan uno de los tres: el plazo de al lado, el órgano vecino, la obligación de otra fase.

Anatomía de una pregunta del ámbito: 80 segundos para reconocer tres datos.

Las cinco trampas del formato

- **La opción más larga.** En los exámenes oficiales la correcta es la más larga solo unas 4 de cada 10 veces: elegir por longitud no aprueba.
- **El absoluto.** «Siempre», «nunca», «en todos los casos» suelen marcar la opción falsa: el Derecho de la Unión vive de excepciones.
- **El actor cambiado.** La obligación está bien descrita pero colgada de otro organismo. Lee el sujeto antes que el verbo.
- **El instrumento vecino.** La afirmación es cierta, pero de otra norma que no aplica a ese caso.
- **El derecho superado.** Redacciones anteriores a una modificación. Estudia siempre texto consolidado.

La ficha que sí sirve

A quién se aplica	Qué obliga	Plazos y cifras	Quién vigila
entidades · productos	la conducta exacta	24 h · 72 h · umbral	y quién sanciona

La ficha por instrumento: cuatro columnas y nada más. Es lo que se contesta en 80 segundos.

4 · El temario, bloque a bloque

El Anexo II describe funciones, no materias. Aquí están traducidas a bloques de estudio: qué entra, qué se confunde y dónde está escrito. Lo que no aparece en un texto oficial no se pregunta.



El ámbito 1 examina el ciclo completo: diseñar, desplegar y gobernar sistemas de IA en una institución.

1 · Diseño, construcción y explotación de soluciones de IA

Ámbito y definición

Requisitos de alto riesgo

Modelos de uso general

Ciclo de vida y MLOps

IA generativa: RAG y agentes

Seguridad de la IA

2 · Uso conforme, defendible y escalable

Prácticas prohibidas y riesgo

Transparencia y alfabetización

Gobernanza y calendario

IA fiable y ALTAI

Gestión de riesgos (AI RMF)

Datos personales

Gobernanza del dato

3 · Política y aplicación de políticas

Política de IA de la Unión

Responsabilidad por producto

El Anexo II traducido a bloques de estudio.

1 Ámbito de aplicación y definición de sistema de IA

La pregunta previa a todo: ¿esto es un sistema de IA y le aplica el Reglamento? De aquí salen varias preguntas por examen.

Qué entra

- Definición del artículo 3(1) leída con las directrices C(2025) 5053: sistema basado en máquina, autonomía, adaptabilidad, objetivos explícitos o implícitos, inferencia y salidas que influyen en entornos físicos o virtuales.
- Qué queda fuera por el artículo 2: seguridad nacional y uso militar, investigación y desarrollo científico, pruebas previas a la comercialización, uso personal no profesional y software libre salvo prohibiciones y obligaciones específicas.
- Papeles y su definición: proveedor, responsable del despliegue, importador, distribuidor y representante autorizado.
- El artículo 25 y cuándo un responsable del despliegue pasa a ser proveedor: marca propia, modificación sustancial o cambio de finalidad prevista.
- Calendario del artículo 113 tal como lo dejó el Reglamento 2026/1744.

Lo que más se confunde

- Sistemas que solo optimizan matemáticamente o aplican reglas fijas no infieren en el sentido del artículo 3(1): las directrices lo dicen expresamente.
- Software libre no significa exento: las prohibiciones del artículo 5 se aplican igualmente.

Fuentes: Reglamento (UE) 2024/1689, artículos 2, 3 y 25 · Directrices C(2025) 5053 · Reglamento (UE) 2026/1744

2 Prácticas prohibidas y clasificación de riesgo

No se pregunta la lista: se pregunta si un caso cae dentro, y casi siempre falta un elemento.

Qué entra

- Prácticas del artículo 5 con sus elementos acumulativos: manipulación con distorsión material del comportamiento y daño significativo, explotación de vulnerabilidades, puntuación social, predicción de delitos basada en perfilado, raspado indiscriminado de rostros, reconocimiento de emociones en trabajo y educación, categorización biométrica de datos sensibles e identificación biométrica remota en tiempo real con fines policiales.
- Las excepciones de la identificación biométrica en tiempo real y la autorización judicial o administrativa previa.
- Dos vías al alto riesgo: producto o componente de seguridad cubierto por el anexo I (artículo 6(1)) y casos de uso del anexo III (artículo 6(2)).
- La excepción del artículo 6(3): tarea preparatoria, mejora de una actividad humana previa, detección de patrones o desviaciones sin sustituir la valoración humana; obligación de documentar la evaluación.
- Las directrices C(2025) 5052 y el proyecto de directrices de clasificación de alto riesgo de 2026.

Lo que más se confunde

- El reconocimiento de emociones solo está prohibido en trabajo y educación, con excepciones médicas y de seguridad.
- Estar en el anexo III no basta: el artículo 6(3) puede sacar al sistema del alto riesgo si cumple una de sus condiciones.

Fuentes: Reglamento (UE) 2024/1689, artículos 5 y 6, anexos I y III · Directrices C(2025) 5052

3 Requisitos de alto riesgo y deberes del responsable del despliegue

El bloque más denso y el que más confunde quién cumple qué.

Qué entra

- Requisitos del proveedor, artículo por artículo: gestión de riesgos (9), gobernanza de datos (10), documentación técnica (11 y anexo IV), registros automáticos (12), transparencia e instrucciones de uso (13), vigilancia humana (14) y exactitud, robustez y ciberseguridad (15).
- Sistema de gestión de la calidad del artículo 17 y conservación de documentación del artículo 18.
- Deberes del responsable del despliegue (artículo 26): usar conforme a las instrucciones, encomendar la vigilancia humana a personas con competencia y autoridad, conservar los registros, vigilar el funcionamiento y suspender el uso ante riesgo.
- Evaluación de impacto sobre derechos fundamentales (artículo 27): quién la debe, cuándo se hace y qué contiene.
- Vigilancia poscomercialización (artículo 72) y notificación de incidentes graves (artículo 73).

Lo que más se confunde

- La evaluación de impacto sobre derechos fundamentales es del responsable del despliegue, no del proveedor.
- Los registros del artículo 12 los genera el sistema por diseño; conservarlos es deber del que lo despliega (artículo 19).

Fuentes: Reglamento (UE) 2024/1689, capítulo III, secciones 2 y 3; artículos 72 y 73; anexos IV y VII

4 Modelos de IA de uso general y Código de buenas prácticas

La materia más nueva y, por eso, la más preguntada en convocatorias recientes.

Qué entra

- Obligaciones de todo proveedor de GPAI (artículo 53): documentación técnica, información a proveedores posteriores, política de cumplimiento de derechos de autor y resumen público suficientemente detallado del contenido de entrenamiento.
- Obligaciones adicionales del modelo con riesgo sistémico (artículo 55): evaluación con protocolos estandarizados, pruebas adversarias, mitigación de riesgos, notificación de incidentes graves y protección de ciberseguridad.
- Presunción de riesgo sistémico a partir de 10²⁵ FLOP acumulados y notificación a la Comisión en dos semanas (artículos 51 y 52).
- Código de buenas prácticas de 2025 y sus capítulos de transparencia, derechos de autor y seguridad; qué significa firmarlo y qué no.
- Excepción de los modelos libres y abiertos y hasta dónde llega.

Lo que más se confunde

- Firmar el código no sustituye la obligación legal: es una vía para demostrar cumplimiento.
- Tener riesgo sistémico añade deberes; nunca exime de los del artículo 53.

Fuentes: Reglamento (UE) 2024/1689, capítulo V · Directrices C(2025) 7719 · Código GPAI 2025

5 Transparencia del artículo 50 y alfabetización

Cuatro obligaciones con destinatarios distintos: el error clásico es colgárselas a quien no toca.

Qué entra

- Proveedor: los sistemas que interactúan con personas deben indicarlo (50(1)); las salidas sintéticas se marcan en formato legible por máquina (50(2)).
- Responsable del despliegue: informa del reconocimiento de emociones y de la categorización biométrica (50(3)); revela ultrafalsificaciones y textos generados de interés público (50(4)).
- Excepciones que leen las directrices C(2026) 5054 y el Código de buenas prácticas sobre marcado de contenido generado.
- Artículo 4 tras el Omnibus: proveedores y responsables adoptan medidas que apoyan la alfabetización en IA de su personal; la Comisión y los Estados miembros las respaldan.

Lo que más se confunde

- La redacción antigua del artículo 4 («garantizar un nivel suficiente») ya no es la vigente: hoy es un distractor.
- Marcar la salida sintética es del proveedor; revelar la ultrafalsificación es del que la despliega.

Fuentes: Reglamento (UE) 2024/1689, artículos 4 y 50 · Directrices C(2026) 5054 · Reglamento (UE) 2026/1744

6 Gobernanza, calendario y Omnibus digital

Quién vigila y desde cuándo. Aquí se juegan las preguntas de actor.

Qué entra

- Oficina de IA: supervisa los modelos de uso general y ejecuta el capítulo V.
- Autoridades nacionales de vigilancia del mercado: sistemas de alto riesgo; el SEPD para las instituciones de la Unión.
- Comité de IA, Grupo de expertos científicos y Foro consultivo: coordinación y asesoramiento, sin potestad de supervisión.
- Calendario de aplicación con las fechas movidas por el Reglamento 2026/1744 y los nuevos artículos 75a a 75d sobre operadores de los sistemas del artículo 75(1).
- Sanciones: importes del artículo 99 y régimen propio de los proveedores de GPAI (artículo 101).

Lo que más se confunde

- Los artículos 75a a 75d no se aplican a los proveedores de modelos de uso general: para ellos rigen los artículos 88 a 94 y el 101.
- El Comité de IA no supervisa a nadie: coordina.

Fuentes: Reglamento (UE) 2024/1689, capítulos VII y XII · Reglamento (UE) 2026/1744

7 IA fiable — directrices éticas y ALTAI

Listas cerradas, fáciles de preguntar y fáciles de confundir entre sí.

Qué entra

- Tres componentes de la IA fiable: lícita, ética y robusta.
- Cuatro principios éticos: respeto de la autonomía humana, prevención del daño, equidad y explicabilidad.
- Siete requisitos clave, desde la acción y supervisión humanas hasta la rendición de cuentas.
- ALTAI como autoevaluación voluntaria y sus preguntas de trazabilidad.
- Modalidades de supervisión: human-in-the-loop, on-the-loop e in-command.

Lo que más se confunde

- Los cuatro principios no son los siete requisitos: los distractores mezclan ambas listas.
- La robustez es un componente, no uno de los cuatro principios.

Fuentes: Directrices éticas para una IA fiable (2019) · ALTAI (2020)

8 Marcos de gestión de riesgos — AI RMF, perfil generativo y sesgo

Guías voluntarias que el examen usa como contraste con la obligación legal.

Qué entra

- Las cuatro funciones del AI RMF 1.0: Govern, Map, Measure y Manage, y qué produce cada una.
- Las siete características de confiabilidad y las etapas del ciclo de vida: planificar y diseñar, recopilar y procesar datos, construir y usar el modelo, verificar y validar, desplegar y usar, operar y monitorizar.
- Riesgos de la IA generativa según AI 600-1: confabulación, integridad de la información, seguridad de la información, cadena de valor, configuración humano-IA, privacidad y sesgo dañino.
- Los tres tipos de sesgo de SP 1270: sistémico, estadístico-computacional y humano, y por qué no se corrigen solo con más datos.

Lo que más se confunde

- Las funciones del AI RMF no son las del CSF de ciberseguridad.
- Las acciones de AI 600-1 son sugeridas: presentarlas como obligatorias es el fallo típico.

Fuentes: NIST AI 100-1 · NIST AI 600-1 · NIST SP 1270

9 Seguridad de la IA — ataques adversarios y aplicaciones con modelos de lenguaje

El bloque que conecta con ciberseguridad y el que más crece.

Qué entra

- Taxonomía de NIST AI 100-2 (2025): en IA predictiva, evasión, envenenamiento y ataques a la privacidad; en IA generativa, cadena de suministro, inyección directa e indirecta de instrucciones y uso indebido.
- Clasificación por objetivo del atacante: disponibilidad, integridad, privacidad y abuso.
- OWASP Top 10 para aplicaciones LLM 2025 y su mitigación pareja para cada entrada.
- Las tres capas del marco de ENISA donde se colocan los controles.

Lo que más se confunde

- Inyección directa no es indirecta: cambia quién introduce el texto malicioso.
- Envenenamiento no es evasión: uno actúa en el entrenamiento, el otro en la inferencia.

Fuentes: NIST AI 100-2 · OWASP Top 10 for LLM Applications 2025 · ENISA multilayer framework

10 IA generativa en la organización — RAG, agentes y guardarraíles

Decisiones de arquitectura con consecuencias de control.

Qué entra

- Cuándo basta el prompting, cuándo toca recuperación aumentada, cuándo ajuste fino y cuándo agentes con herramientas.
- El control que exige cada patrón: anclaje y procedencia, tratamiento de la salida, permisos de herramienta y puertas de aprobación, evaluación y pruebas antes del despliegue, y supervisión humana.
- Qué exige el SEPD a una institución de la UE antes de usar IA generativa.
- Registro de decisiones y trazabilidad de las salidas usadas como prueba.

Lo que más se confunde

- La recuperación aumentada no arregla el sesgo: reduce la invención sobre datos propios.
- Un agente sin límite de autorización es un riesgo de seguridad, no una mejora de productividad.

Fuentes: NIST AI 600-1 · OWASP LLM Top 10 2025 · Orientaciones del SEPD (2025)

11 Ciclo de vida, MLOps y vigilancia poscomercialización

La parte de ingeniería del Anexo II, con los artefactos que exige la norma.

Qué entra

- Secuencia del ciclo de vida y qué evidencia deja cada etapa.
- Artefactos que mantienen auditable un sistema de alto riesgo: registros automáticos (artículo 12) con la conservación del artículo 19, sistema de gestión de la calidad (17), plan de vigilancia poscomercialización (72) e informes de incidente grave (73).
- Prácticas de desarrollo seguro para IA generativa (SP 800-218A) y su encaje con el SSDF.
- Modelos de servicio y despliegue en la nube (SP 800-145) y responsabilidad compartida (SP 800-144).

Lo que más se confunde

- El despliegue no cierra el ciclo: la vigilancia poscomercialización es obligación continua del proveedor.
- Externalizar a la nube no externaliza la responsabilidad del responsable del despliegue.

Fuentes: Reglamento (UE) 2024/1689, artículos 12, 17, 19, 72 y 73 · NIST SP 800-218A · SP 800-144 y 800-145

12 Datos personales en la IA

Donde el Reglamento de IA se cruza con protección de datos, con una norma distinta para las instituciones.

Qué entra

- Dictamen 28/2024 del CEPD: cuándo un modelo puede considerarse anónimo y qué hay que demostrar.
- La prueba de interés legítimo en tres pasos: interés legítimo, necesidad y ponderación.
- Consecuencias del desarrollo ilícito de un modelo sobre su uso posterior.
- Instituciones de la UE: se rigen por el Reglamento 2018/1725, que no tiene base de interés legítimo; papel del delegado de protección de datos y de la evaluación de impacto.
- Categorías especiales para detección de sesgos: tras el Omnibus, la puerta está en el nuevo artículo 4a, no en el 10(5).

Lo que más se confunde

- Citar artículos del RGPD para una institución europea es un error de norma, no de detalle.
- Anonimato de un modelo no se presume: se justifica.

Fuentes: Dictamen CEPD 28/2024 · Reglamento (UE) 2018/1725 · Orientaciones del SEPD 2025 · Reglamento (UE) 2026/1744

13 Gobernanza del dato para la IA

Preparación del dato según el Anexo II, con tres instrumentos que no hay que mezclar.

Qué entra

- Artículo 10 del Reglamento de IA: prácticas de gobernanza para datos de entrenamiento, validación y prueba; decisiones de diseño, recogida, examen de sesgos y detección de lagunas.
- Reglamento de Datos 2023/2854: datos de productos conectados, acceso de organismos públicos y cambio de proveedor de servicios de tratamiento.
- Reglamento de Gobernanza de Datos 2022/868: reutilización de datos protegidos del sector público, servicios de intermediación y altruismo de datos.
- Qué exigir por contrato a un proveedor de datos de entrenamiento.

Lo que más se confunde

- El Reglamento de Datos no es una norma de protección de datos: regula acceso y uso.
- El artículo 10 no exige datos perfectos: exige pertinencia, representatividad y, en la medida de lo posible, ausencia de errores.

Fuentes: Reglamento (UE) 2024/1689, artículo 10 · Reglamento (UE) 2023/2854 · Reglamento (UE) 2022/868

14 Responsabilidad por producto y seguridad

Bloque corto con fecha propia y consecuencias prácticas.

Qué entra

- La Directiva 2024/2853 trata el software y los sistemas de IA como producto (artículo 4) y excluye el software libre suministrado fuera de una actividad comercial (artículo 2(2)).
- Quién responde a lo largo de la cadena (artículo 8) y qué pasa con la modificación sustancial fuera del control del fabricante.
- Test de carácter defectuoso, incluido el aprendizaje posterior a la puesta en el mercado (artículo 7).
- Divulgación de pruebas y presunciones (artículos 9 y 10); defensa del riesgo de desarrollo y su excepción (artículos 11 y 18); plazos de prescripción y caducidad (16 y 17).
- Fecha de aplicación: 9 de diciembre de 2026.

Lo que más se confunde

- Cumplir el Reglamento de IA no excluye la responsabilidad civil por producto defectuoso.
- La exclusión del software libre no alcanza al suministrado en el marco de una actividad comercial.

Fuentes: Directiva (UE) 2024/2853

15 Política de IA de la Unión

Preguntas de atribución: qué iniciativa pertenece a qué instrumento.

Qué entra

- Fábricas de IA bajo el Reglamento EuroHPC modificado (2024/1732).
- Gigafábricas de IA e InvestAI en el Plan del Continente de la IA (COM(2025) 165) y sus cinco áreas.
- Política de «IA primero» y buques insignia sectoriales de la Estrategia Apply AI (COM(2025) 723).
- RAISE en la estrategia de IA en la ciencia (COM(2025) 724).
- Libro Blanco de 2020 (ecosistemas de excelencia y de confianza) y revisión del Plan coordinado de 2021.
- Reglamento de Europa Interoperable (2024/903): evaluación de interoperabilidad y Consejo de Europa Interoperable.

Lo que más se confunde

- Las fábricas de IA no salen del Reglamento de IA: salen de EuroHPC.
- El Plan del Continente y la Estrategia Apply AI son documentos distintos con objetivos distintos.

Fuentes: COM(2020) 65 · COM(2021) 205 · COM(2025) 165, 723 y 724 · Reglamentos (UE) 2024/1732 y 2024/903

5 · Cómo estudiarlo en ocho semanas



Ocho semanas dan para dos vueltas al temario si se contesta desde el principio.

semana	1	2	3	4	5	6	7	8
Mapa y fichas								
Estudio por bloques								
Bloques flojos y cifras								
Simulacros cronometrados								
Repaso y razonamiento								

Reparto: dos tercios al ámbito y un tercio al razonamiento. El ámbito ordena; el razonamiento solo elimina. Y desde la semana 3, preguntas el mismo día que se estudia el bloque: leer sin contestar no fija nada.

6 · Biblioteca oficial

Todo lo que sigue es público y citable. Ninguna preparación sería necesita más, y ningún manual comercial sustituye al texto consolidado.

Documento	Para qué
Reglamento (UE) 2024/1689 — Reglamento de IA, texto consolidado	La norma central; leerla con las modificaciones del Omnibus incorporadas.
Reglamento (UE) 2026/1744 — Omnibus digital	Qué artículos cambiaron y desde cuándo; incluye los nuevos 4a y 75a-75d.
Directrices C(2025) 5053 · C(2025) 5052 · C(2026) 5054 · C(2025) 7719	Definición de sistema de IA, prácticas prohibidas, transparencia del artículo 50 y obligaciones GPAI.
Código de buenas prácticas GPAI 2025	Capítulos de transparencia, derechos de autor y seguridad.
Directrices éticas para una IA fiable (2019) y ALTAI (2020)	Componentes, principios, siete requisitos y autoevaluación.
NIST AI 100-1 · AI 600-1 · AI 100-2 · SP 1270	Gestión de riesgos, IA generativa, ataques adversarios y sesgo.
OWASP Top 10 for LLM Applications 2025	

Documento	Para qué
	Riesgos de aplicaciones con modelos de lenguaje, RAG y agentes.
ENISA — marco multicapa de ciberseguridad de la IA (2023)	Cómo se ordenan los controles de seguridad de un sistema de IA.
NIST SP 800-218A · SP 800-144 · SP 800-145 · SP 800-146	Desarrollo seguro con IA generativa y computación en la nube.
Dictamen 28/2024 del CEPD y orientaciones del SEPD (2025)	Datos personales en modelos y uso de IA generativa en instituciones de la UE.
Reglamentos 2023/2854, 2022/868, 2024/903 y 2024/1732	Datos, gobernanza del dato, interoperabilidad y EuroHPC.
Directiva (UE) 2024/2853	Responsabilidad por productos defectuosos, software incluido.

7 · Antes de darte por preparado

- De un caso cualquiera: ¿es sistema de IA, de qué riesgo y quién responde?
- ¿Separas sin dudar las obligaciones del proveedor de las del responsable del despliegue?
- ¿Manejas el calendario del artículo 113 después del Omnibus, no el original?
- ¿Distingues guía voluntaria (NIST, ALTAI) de obligación legal?
- ¿Sitúas Oficina de IA, autoridades nacionales y SEPD sin confundir competencias?
- ¿Sabes qué cambió el Omnibus en los artículos 4, 10(5) y 75a-75d?
- ¿Has hecho tres simulacros de 30 preguntas en 40 minutos, en tu lengua 2?

Practica con preguntas de este ámbito, en los cinco idiomas del examen.

Banco de inteligencia artificial de EPSO/AD/430/26, con la explicación y el artículo detrás de cada respuesta: eu-now.com/specialist/artificial-intelligence



Y cuando algo falle, pregúntalo. En EU-now, EUgenio responde con la norma delante y cita el artículo del que sale la respuesta: es la diferencia entre saber que fallaste y saber por qué.

Cifras y plazos proceden de la convocatoria publicada en el Diario Oficial (C/2026/4668) y de los textos oficiales citados. Si EPSO publica una corrección de errores, manda el Diario Oficial.