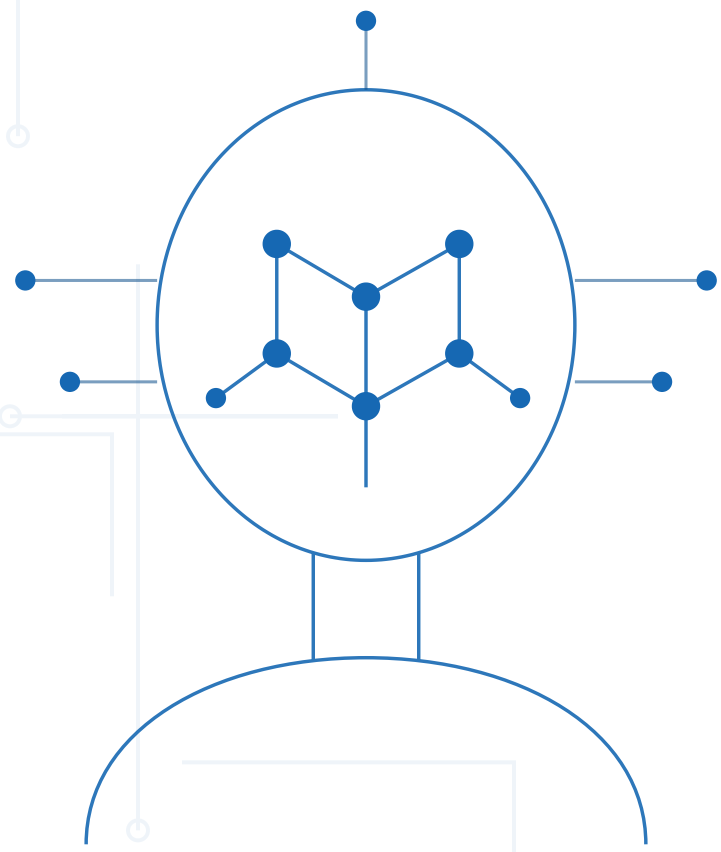
GRCreal

REGLAMENTO EUROPEO DE INTELIGENCIA ARTIFICIAL

Versión 1.0 · Agosto 2026

AI Act — Reglamento (UE) 2024/1689, modificado por el Reglamento (UE) 2026/1744

Documento de arranque del proyecto de adecuación



ELABORADO POR

Miguel Ángel Carriazo

GRCReal · OpenTrust.Group

RIESGO · TRANSPARENCIA · GOBERNANZA · EVIDENCIA · PLAZOS

1 OBJETIVO DEL PROYECTO

Por qué ahora

El Reglamento (UE) 2024/1689 está en vigor desde agosto de 2024 y ya tiene obligaciones exigibles. El Ómnibus digital no ha suspendido el Reglamento: ha movido fechas concretas.

Qué debe decidir el proyecto

Alcance, roles, responsables y forma de trabajo. El arranque debe dejar un responsable designado y el inventario abierto.

Qué no es este proyecto

No es un informe jurídico ni un PDF que se archiva. Es una capacidad operativa: inventario vivo, clasificación defendible y evidencia recuperable.

La regla de la casa

Lo que no se puede demostrar, no se cumple. Toda decisión de este proyecto queda escrita, fechada y firmada.

Resultado inicial esperado

Responsable de IA designado · lista inicial de sistemas · fecha del primer comité · criterio de clasificación acordado.

2 EL MARCO: REGLAMENTO (UE) 2024/1689

Qué es

La primera norma horizontal del mundo sobre inteligencia artificial. Es un **reglamento**: aplicación directa en los 27 Estados, sin trasposición nacional.

Cómo regula

Por **riesgo** y por **uso**, no por tecnología. La misma herramienta puede ser de riesgo mínimo o de alto riesgo según para qué se emplee y sobre quién decida.

Qué es un sistema de IA

Sistema automatizado con cierto grado de autonomía que infiere, a partir de las entradas que recibe, cómo generar salidas — predicciones, contenidos, recomendaciones o decisiones — capaces de influir en entornos físicos o virtuales.

Alcance territorial

Aplica a quien pone el sistema en el mercado o en servicio en la UE y también a proveedores de fuera cuando el resultado se utiliza dentro de la Unión. Estar fuera no es estar exento.

Exclusiones

Uso personal no profesional, investigación y desarrollo previos a la comercialización,
fines militares y de defensa, y determinados sistemas publicados bajo licencia libre y de
código abierto, con las excepciones previstas. La exclusión debe justificarse.

3 QUÉ HA CAMBIADO: EL ÓMNIBUS DIGITAL

Reglamento (UE) 2026/1744

De 8 de julio de 2026, publicado en el DOUE el 24 de julio y en vigor desde el **27 de julio de 2026**. Primera reforma del AI Act desde su adopción.

No es una moratoria

La arquitectura no se toca: enfoque de riesgo, cuatro categorías, reglas de GPAI y supervisión europea siguen igual. Lo que se ha reordenado son los plazos del alto riesgo.

Lo que sí se aplaza

Alto riesgo del **Anexo III**: del 2 de agosto de 2026 al **2 de diciembre de 2027**. Alto riesgo del **Anexo I** (embebido en producto): al **2 de agosto de 2028**. Sandboxes nacionales: a agosto de 2027.

Lo que se añade

Nueva práctica prohibida: sistemas que generan contenido íntimo no consentido y material de abuso sexual infantil. Además, simplificación para pymes y midcaps y ajustes en registro y alfabetización.

El titular es medio falso

«El AI Act se ha retrasado» es la mitad peligrosa de la verdad. La transparencia del artículo 50 aplica desde el 2 de agosto de 2026. Ya está vigente.

4 CALENDARIO DE APLICACIÓN

1 ago 2024	Entrada en vigor del Reglamento	HECHO
2 feb 2025	Prácticas prohibidas (art. 5) y alfabetización en IA (art. 4)	VIGENTE
2 ago 2025	Modelos de propósito general (GPAI), gobernanza, autoridades y régimen sancionador	VIGENTE
2 ago 2026	Aplicación general: transparencia (art. 50), multas a GPAI (art. 101), registro y notificación	VIGENTE
2 dic 2026	Transición del marcado de contenido sintético · prohibición de «nudificadores» y CSAM	PRÓXIMO
2 ago 2027	Sandboxes regulatorios nacionales · GPAI comercializados antes de agosto de 2025	FUTURO
2 dic 2027	Alto riesgo del Anexo III y evaluación de impacto en derechos fundamentales (art. 27)	APLAZADO
2 ago 2028	Alto riesgo del Anexo I: IA embebida en productos regulados	APLAZADO

Dónde estamos hoy

A 22 de agosto de 2026 ya son exigibles las prohibiciones, la alfabetización, las obligaciones de GPAI y la transparencia del artículo 50. El margen que queda es para el alto riesgo, y solo para eso.

5 A QUIÉN APLICA: LOS ROLES

Proveedor (provider)

Desarrolla o encarga desarrollar un sistema de IA y lo pone en el mercado o en servicio bajo su nombre o marca. Soporta la carga máxima de obligaciones.

Responsable del despliegue (deployer)

Utiliza el sistema bajo su propia autoridad en el ejercicio de su actividad profesional. Es el papel de la inmensa mayoría de las organizaciones.

Importador, distribuidor y representante autorizado

Cadena de suministro: verificación documental, marcado CE, conservación de documentación y cooperación con las autoridades.

Artículo 25: el cambio de rol

Pasas a ser proveedor si pones tu marca en un sistema de alto riesgo, lo modificas
sustancialmente o cambias su finalidad prevista. Fine-tuning y rebranding deben evaluarse:
si implican una modificación sustancial o un cambio de finalidad, pueden provocar un cambio de rol.

Primera decisión del proyecto

Determinar el rol por cada sistema. Cambia la lista completa de obligaciones y el coste del cumplimiento.

6 LAS CUATRO CATEGORÍAS DE RIESGO

Riesgo inaceptable

Prácticas prohibidas del artículo 5. No hay medida compensatoria posible: no se despliegan. Multa máxima del Reglamento.

Alto riesgo

Anexo III (por uso) y Anexo I (embebido en producto). Requisitos completos: gestión de riesgos, datos, documentación, supervisión humana, robustez y evaluación de conformidad.

Riesgo limitado — transparencia

Chatbots, generadores de contenido y deepfakes. Obligaciones de transparencia según el supue
El reconocimiento de emociones requiere una clasificación específica según el contexto.
Vigente desde agosto de 2026.

Riesgo mínimo

El grueso de las aplicaciones: filtros de spam, recomendadores internos, optimización. Sin obligaciones específicas, con buenas prácticas voluntarias.

La clasificación no es una opinión

Hay que documentarla, fecharla y firmarla. Es la primera pieza que pedirá un auditor, un cliente o un inspector. Sobre ella se apoya todo lo demás.

7 PRÁCTICAS PROHIBIDAS (ART. 5)

- **Manipulación subliminal** o técnicas deliberadamente engañosas que distorsionen el comportamiento y causen un perjuicio significativo.
- **Explotación de vulnerabilidades** por edad, discapacidad o situación social o económica.
- **Puntuación social** que derive en trato perjudicial o desproporcionado fuera del contexto en que se obtuvieron los datos.
- **Predicción de delitos** basada exclusivamente en perfilado o en rasgos de personalidad.
- **Extracción masiva e indiscriminada de imágenes faciales** de internet o de circuitos de videovigilancia para crear bases de reconocimiento.
- **Reconocimiento de emociones** en el lugar de trabajo y en centros educativos, salvo por motivos médicos o de seguridad.
- **Categorización biométrica** para inferir raza, opiniones políticas, afiliación sindical, creencias religiosas, vida u orientación sexual.
- **Identificación biométrica remota en tiempo real** en espacios públicos con fines policiales, salvo supuestos tasados y con autorización judicial.
- **Nuevo (2 dic 2026):** generación de contenido íntimo no consentido y de material de abuso sexual infantil.

Consecuencia

Hasta **35 millones de euros** o el **7 %** del volumen de negocio mundial anual, la cifra que sea mayor.

8 ALTO RIESGO: ANEXO III

- **Biometría** — identificación remota, categorización biométrica y reconocimiento de emociones fuera de los supuestos prohibidos.
- **Infraestructuras críticas** — componentes de seguridad en la gestión y operación de tráfico, agua, gas, calefacción, electricidad e infraestructuras digitales críticas.
- **Educación y formación** — admisión, evaluación de resultados, orientación del itinerario y detección de fraude en exámenes.
- **Empleo y gestión de trabajadores** — selección, filtrado de currículos, promoción, extinción, asignación de tareas y monitorización del rendimiento.
- **Servicios esenciales** — acceso a prestaciones públicas, evaluación de solvencia, precios y riesgo en seguros de vida y salud, y triaje de emergencias.
- **Aplicación de la ley** — evaluación de fiabilidad de pruebas, perfilado y valoración del riesgo de delinquir.
- **Migración, asilo y control fronterizo** — verificación de documentos y examen de solicitudes.
- **Justicia y procesos democráticos** — apoyo a la interpretación del derecho y sistemas que influyen en el resultado electoral.

Dónde aparece de verdad en una empresa media

Recursos Humanos, scoring de clientes y control de acceso biométrico. Ese es el trío que hay que mirar primero en el inventario.

9 ALTO RIESGO: ANEXO I Y EXCEPCIONES

Anexo I — IA embebida en producto

Sistemas incorporados a productos ya cubiertos por legislación armonizada: máquinas, ascensores, juguetes, dispositivos médicos, automoción, aviación. La conformidad se integra en la del producto.

Artículo 6.3 — el filtro

Un sistema del Anexo III no es de alto riesgo si solo realiza una tarea procedimental limitada, mejora el resultado de una actividad humana previa, detecta patrones de decisión sin sustituir la valoración humana, o es meramente preparatorio.

El filtro tiene precio

Quien lo invoque debe **documentar la evaluación** antes de poner el sistema en el mercado y registrarlo. Y si el sistema realiza perfilado de personas físicas, la excepción no está disponible.

> **Aviso**
>
> La excepción del 6.3 se usa mucho y se documenta poco. Es exactamente el punto por donde se pierde una inspección.

10 REQUISITOS DE LOS SISTEMAS DE ALTO RIESGO

Gestión de riesgos (art. 9)

Proceso continuo e iterativo durante todo el ciclo de vida: identificación, estimación, medidas de mitigación y pruebas. No es un documento anual.

Gobernanza de datos (art. 10)

Calidad, pertinencia y representatividad de los conjuntos de entrenamiento, validación y prueba. Examen de sesgos y trazabilidad del origen del dato.

Documentación y registros (arts. 11-12)

Documentación técnica conforme al Anexo IV y registro automático de eventos (logs), con conservación mínima de seis meses.

Supervisión humana y robustez (arts. 13-15)

Instrucciones de uso claras, capacidad real de intervenir y detener el sistema, precisión declarada, resiliencia y ciberseguridad frente a manipulación de datos y del modelo.

Y encima de todo eso

Sistema de gestión de la calidad (art. 17), evaluación de conformidad, declaración UE, marcado CE y registro en la base de datos europea.

11 OBLIGACIONES DEL PROVEEDOR

- Implantar un **sistema de gestión de la calidad** documentado y proporcionado a la organización.
- Elaborar y conservar la **documentación técnica** y los registros durante **diez años** desde la comercialización.
- Superar la **evaluación de conformidad** aplicable, emitir la declaración UE y colocar el **marcado CE**.
- **Registrar** el sistema en la base de datos de la UE antes de ponerlo en el mercado o en servicio.
- Mantener un plan de **vigilancia poscomercialización** que recoja el comportamiento real del sistema.
- **Notificar incidentes graves** a la autoridad de vigilancia: regla general 15 días; 2 días si hay infracción generalizada o riesgo grave; 10 días en caso de fallecimiento.
- Adoptar **medidas correctoras** inmediatas, informar a la cadena de distribución y cooperar con las autoridades.
- Designar **representante autorizado** en la UE si el proveedor está establecido fuera.

> ⚠ **Trampa habitual**
>
> Si contratas un sistema de alto riesgo y le pones tu marca, eres proveedor. Con todo lo anterior encima.

12 OBLIGACIONES DEL RESPONSABLE DEL DESPLIEGUE

- Utilizar el sistema **conforme a las instrucciones de uso** del proveedor. Desviarse de ellas te acerca al artículo 25.
- Asignar la **supervisión humana** a personas con competencia, formación y **autoridad real** para intervenir o parar el sistema.
- Garantizar que los **datos de entrada** bajo su control son pertinentes y suficientemente representativos.
- Conservar los **registros automáticos** durante al menos seis meses cuando estén bajo su control.
- **Informar a los trabajadores** y a sus representantes antes de poner en servicio IA de alto riesgo en el entorno laboral.
- **Informar a las personas** sujetas a decisiones tomadas o asistidas por el sistema, y atender su derecho a explicación.
- **Vigilar** el funcionamiento, suspender el uso ante riesgo y notificar incidentes graves al proveedor y a la autoridad.
- Realizar la evaluación de impacto en derechos fundamentales (FRIA) cuando resulte exigible: organismos de Derecho público, entidades privadas que presten servicios públicos y determinados
sistemas de credit scoring y seguros de vida y salud.

Lo que no se puede subcontratar

La supervisión humana es del deployer. El proveedor la habilita; tú la ejerces. Un humano de adorno junto al botón no cumple el artículo 14.

13 TRANSPARENCIA (ART. 50): LO QUE YA OBLIGA

Interacción con personas

Si el sistema conversa con personas, hay que informar de que se está tratando con una IA, salvo que resulte evidente para un usuario razonablemente atento.

Contenido sintético

El audio, la imagen, el vídeo y el texto generados o manipulados por IA deben marcarse en un formato **legible por máquina** y ser detectables como artificiales.

Deepfakes y texto de interés público

Divulgación explícita de que el contenido ha sido generado o manipulado. En texto informativo, salvo que exista revisión editorial humana con responsabilidad identificada.

Emociones y biometría

Los sistemas de reconocimiento de emociones o de categorización biométrica deben informar a las personas expuestas, con la base jurídica de protección de datos que corresponda.

Fecha

Aplica desde el **2 de agosto de 2026**. No se aplazó. Si hay un chatbot en la web o se genera contenido con IA, esto ya obliga.

14 MARCADO DE CONTENIDO SINTÉTICO

Dos capas, no una

Etiqueta **visible** para la persona que consume el contenido y marca **legible por máquina** incrustada: metadatos, marca de agua o huella digital.

Cómo debe ser

Eficaz, interoperable, robusta y fiable en la medida en que sea técnicamente viable. El listón es el estado del arte, no la buena intención.

Dónde toca de verdad

En el pipeline de generación, en el gestor de contenidos, en la biblioteca de medios y en los contratos con agencias y proveedores externos.

Referencias técnicas

C2PA / Content Credentials, marcas de agua a nivel de modelo y metadatos IPTC. Conviene fijar un estándar antes de tener veinte flujos distintos.

Realidad de calendario

Esto son meses de ingeniería y de acuerdos con proveedores. Arrancarlo en noviembre es llegar tarde.

15 MODELOS DE PROPÓSITO GENERAL (GPAI)

Obligaciones vigentes desde agosto de 2025

Documentación técnica del modelo, información suficiente para quien lo integre, política de cumplimiento de derechos de autor y resumen público de los datos de entrenamiento.

Modelos con riesgo sistémico

Umbral indicativo de 10^{25} FLOP de cómputo de entrenamiento. Añade evaluaciones adversariales, mitigación de riesgos, ciberseguridad reforzada y notificación de incidentes graves.

Código de buenas prácticas

Mientras faltan normas armonizadas, adherirse al código de GPAI es la vía práctica para demostrar cumplimiento ante la Oficina Europea de IA.

Qué significa para nosotros

Integrar modelos de terceros no nos convierte en proveedores de GPAI, pero **necesitamos su documentación**. Eso es una cláusula contractual, no un favor del comercial.

Sanción específica

Hasta 15 millones de euros o el 3 % del volumen de negocio mundial, impuesta directamente por la Comisión. Aplicable desde agosto de 2026.

16 ALFABETIZACIÓN EN IA (ART. 4)

Vigente desde febrero de 2025

Proveedores y responsables del despliegue deben adoptar medidas para apoyar el desarrollo de la alfabetización en IA del personal y de quienes operen o utilicen estos sistemas en su nombre, atendiendo a conocimientos, experiencia, formación, contexto de uso y personas afectadas.

Proporcional, no genérica

Se calibra según el rol, el conocimiento previo, el contexto de uso y las personas sobre las que el sistema produce efectos.

Cómo se demuestra

Itinerarios diferenciados por perfil — dirección, negocio, técnico, jurídico, RR. HH. — con contenidos, asistentes, fechas y evaluación registrados.

Qué cambió con el Ómnibus

El Reglamento no exige garantizar un nivel concreto de competencia de cada individuo, pero sí
adoptar y poder demostrar medidas proporcionadas de alfabetización en IA.

Lectura práctica

Es el incumplimiento más fácil de detectar en una inspección y el más barato de resolver. No hay excusa razonable para no tenerlo.

17 RÉGIMEN SANCIONADOR

- **Prácticas prohibidas (art. 5):** hasta **35 M€** o el **7 %** del volumen de negocio mundial anual total, la cifra superior.
- **Incumplimiento del resto de obligaciones** — alto riesgo, transparencia, deployers, importadores, organismos notificados: hasta **15 M€** o el **3 %**.
- **Información incorrecta, incompleta o engañosa** a autoridades u organismos notificados: hasta **7,5 M€** o el **1 %**.
- **Proveedores de GPAI:** hasta **15 M€** o el **3 %**, impuestas directamente por la Comisión Europea.
- **Pymes y startups:** se aplica el importe **menor** de los dos porcentajes o cifras.
- **Criterios de graduación:** gravedad y duración, número de afectados, intencionalidad, medidas correctoras adoptadas, cooperación y reincidencia.
- Las autoridades pueden además **retirar del mercado** el sistema o prohibir su uso, con impacto operativo superior al de la multa.

Sin periodo de gracia

El régimen sancionador general aplica desde el 2 de agosto de 2025; las multas a proveedores de GPAI, desde agosto de 2026.

18 SUPERVISIÓN Y AUTORIDADES

Oficina Europea de IA

Supervisa a los proveedores de modelos de propósito general, coordina la aplicación del Reglamen y publica directrices y códigos de práctica. Tras la reforma de 2026, asume además competencias directas sobre determinados sistemas basados en GPAI.

Estructura europea

Comité Europeo de Inteligencia Artificial, panel científico de expertos independientes y foro consultivo de partes interesadas.

En España

La **AESIA**, con sede en A Coruña, como autoridad de vigilancia del mercado, junto a AEPD, Banco de España, CNMV y CNMC en sus respectivos ámbitos sectoriales.

Sandbox regulatorio

España fue pionera en poner en marcha un entorno controlado de pruebas. Los sandboxes obligatorios en todos los Estados pasan a agosto de 2027.

Preparación mínima

Interlocutor designado y expediente localizable antes de recibir el primer requerimiento. Improvisar la respuesta sale caro y deja rastro.

19 ENCAJE CON EL RESTO DEL MARCO

ISO/IEC 42001

El AI Act dice **qué**; la 42001 aporta el **cómo**: sistema de gestión de IA con responsables, procesos, evidencias y ciclo de mejora. Lo que la 27001 hizo con la seguridad.

ISO/IEC 27001 y ENS

La ciberseguridad exigida por el artículo 15 no se inventa desde cero: se apoya en los controles, la gestión de activos y la respuesta a incidentes que ya existen.

RGPD

Base jurídica, minimización, decisiones automatizadas del artículo 22 y derechos de las personas. La FRIA no sustituye a la evaluación de impacto de protección de datos: se complementan.

NIS2 y DORA

Notificación de incidentes y gestión del riesgo de terceros. Un único registro de proveedores y un único flujo de notificación, no cuatro en paralelo.

Principio de diseño

Un solo sistema de gestión, varios marcos encima. Duplicar controles multiplica el coste y fragmenta la evidencia.

20 EL PROYECTO: ENFOQUE Y PRINCIPIOS

Entender antes de cumplir

Ningún sistema se clasifica sin conocer su uso real, quién decide con él y sobre quién produce efectos. La clasificación de despacho se cae en la primera pregunta.

Riesgo en términos de negocio

El impacto se expresa en consecuencias reales — jurídicas, operativas, reputacionales — no en colores de una matriz.

Ejecutar, no documentar

Cada fase entrega algo utilizable: un inventario que se consulta, un registro que se firma, un control que funciona. El documento es el residuo, no el objetivo.

Mantener

Inventario y clasificación se revisan con cadencia fija. Un sistema nuevo sin clasificar es una brecha abierta desde el día uno.

Traducción operativa

Seis fases, responsables nominales por fase y un único repositorio de evidencia desde el primer día.

21 FASES 1 A 3

Fase 1 · Descubrimiento e inventario — semanas 1-3

Censo de sistemas propios, IA embebida en SaaS y **shadow AI**. Ficha por sistema: finalidad, datos que trata, proveedor, rol, usuarios, decisiones que soporta y criticidad.

Fase 2 · Clasificación y rol — semanas 3-5

Categoría de riesgo y rol de la organización por cada sistema, con justificación escrita, fecha y firma. Aplicación razonada del filtro del artículo 6.3 donde proceda.

Fase 3 · Análisis de brechas — semanas 5-8

Contraste contra los requisitos aplicables **según su fecha exigible**. Salida: mapa de brechas priorizado por exposición real y esfuerzo de cierre.

Riesgo de estas tres fases

El inventario incompleto. Lo que no aparece en la lista no se clasifica, no se controla y aparece solo cuando falla.

22 FASES 4 A 6

Fase 4 · Plan de adecuación — semanas 8-10

Acciones concretas con responsable, fecha y coste. Se prioriza por fecha exigible y exposición, no por facilidad de ejecución.

Fase 5 · Implantación — semanas 10-24

Políticas y procedimientos, supervisión humana operativa, controles técnicos, marcado de contenido, cláusulas contractuales con proveedores y formación por perfil.

Fase 6 · Operación y vigilancia — continuo

Comité periódico, revisión del inventario, monitorización del comportamiento en producción, gestión de incidentes y preparación permanente de auditoría.

Criterio de cierre de fase

Una fase se cierra cuando su evidencia puede enseñarse a un tercero sin preparación previa. No cuando el documento está escrito.

23 ENTREGABLES Y EVIDENCIAS

- **Inventario de sistemas de IA** vivo, con responsable nominal por sistema y fecha de última revisión.
- **Registro de clasificación** con justificación, criterio aplicado, firma y control de versiones.
- **Política de uso de IA** y código ético: usos permitidos, prohibidos y condicionados.
- **Mapa de brechas y plan de adecuación** con seguimiento periódico y estado por acción.
- **Procedimiento de supervisión humana**: quién, con qué autoridad, con qué criterio de intervención.
- **Procedimiento de incidentes de IA** conectado con el flujo existente de seguridad.
- **Cláusulas contractuales** para proveedores de IA y de modelos: documentación, marcado, notificación y auditoría.
- **Plan de formación y registro de alfabetización** por perfil, con evidencia de asistencia.
- **Expediente por sistema**: toda la evidencia recuperable en minutos, no en semanas.

Criterio de aceptación

Si no se puede enseñar, no cuenta. Si no tiene fecha y responsable, no es evidencia.

24 GOBERNANZA, RIESGOS Y PRÓXIMOS PASOS

Gobernanza del proyecto

Patrocinador de dirección, responsable de IA, comité mensual y puntos de contacto en negocio, TI, jurídico, RR. HH. y seguridad. Sin patrocinio real, el inventario no se completa.

Riesgos del proyecto

Falsa calma por el aplazamiento · shadow AI fuera del inventario · clasificación optimista para evitar trabajo · dependencia de documentación que el proveedor no entrega · formación tratada como casilla.

Factores críticos de éxito

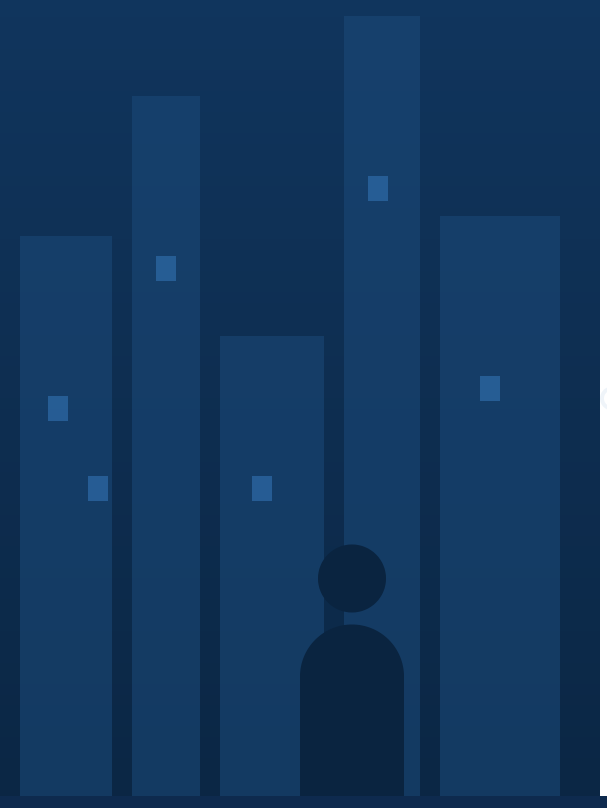
Acceso a los dueños de proceso, decisiones registradas, un único repositorio de evidencia y cadencia fija de revisión.

Próximos pasos — esta semana

Designar responsable de IA · abrir el inventario y repartir las fichas · fijar la fecha del primer comité · acordar el criterio de clasificación.

El aplazamiento no es tiempo regalado.
Es el único margen que vas a tener para llegar preparado.

Cumplir es una decisión. Demostrarlo es un sistema.



INVENTARIO CLASIFICACIÓN EVIDENCIA CONTINUIDAD

GRCreal OpenTrust.Group