J2DINTELLIGENCE · SECTOR PÚBLICO

Qué exigir a un proveedor de IA en una licitación

Diez requisitos para el pliego, con su justificación, una cláusula tipo y la evidencia que conviene pedir al licitador.

Octubre 2026 · Versión 1.0
Incluye los cambios del Ómnibus Digital de IA (Reglamento (UE) 2026/1744), en vigor desde el 27 de julio de 2026.

Documento de uso libre: puede copiarse y adaptarse a cualquier pliego.

Para quién es y cómo usarlo

Este documento está pensado para quien prepara o informa un expediente de contratación que incluye un sistema de inteligencia artificial: personal técnico de las áreas promotoras, responsables de contratación, de sistemas de información y de protección de datos, secretarías e intervenciones. También sirve para valorar ofertas y para revisar contratos que ya están en ejecución. Recoge los diez puntos que, si no figuran en el pliego, difícilmente se exigirán en la ejecución.

Cada requisito se presenta con la misma estructura: qué exigir, por qué, cómo redactarlo en el pliego (con una cláusula tipo) y qué evidencia pedir al licitador. Las cláusulas son orientativas: deben adaptarse al objeto y al importe del contrato, a la categoría del sistema en el Esquema Nacional de Seguridad y al procedimiento elegido, y revisarse con los servicios jurídicos del órgano de contratación. Al final se incluye una lista de comprobación de una página para usar al redactar. El documento puede copiarse y adaptarse libremente.

> **Tres criterios antes de copiar ninguna cláusula**
>
> **Proporcionalidad.** No pesa lo mismo un contrato menor de formación que un sistema que trata expedientes con datos sensibles. Los requisitos deben guardar relación con el objeto del contrato y con el riesgo real del tratamiento.
>
> **Concurrencia.** Cuando se exijan certificaciones, hay que admitir certificados equivalentes y otras pruebas de medidas equivalentes. Un requisito desproporcionado no protege más: reduce el número de ofertas.
>
> **Ubicación en el pliego.** Cada requisito puede ir en la solvencia técnica, en las prescripciones técnicas, en los criterios de adjudicación o en las condiciones especiales de ejecución. Junto a cada cláusula se indica dónde suele encajar mejor.

Contenido

1. El marco normativo, en breve
2. Los diez requisitos
   - 01 · Tratamiento exclusivo en el Espacio Económico Europeo
   - 02 · Contrato de encargado del tratamiento
   - 03 · Compromiso de no entrenar modelos con la información
   - 04 · Conformidad con el Esquema Nacional de Seguridad
   - 05 · Certificaciones de seguridad de la información
   - 06 · Trazabilidad completa
   - 07 · Supervisión humana definida
   - 08 · Descripción técnica, riesgos y clasificación
   - 09 · Borrado verificable
   - 10 · Propiedad del resultado y salida sin dependencias
3. Lista de comprobación para el pliego
4. Aviso y contacto

El marco normativo, en breve

El Reglamento europeo de IA se aplica ya, sin esperar a ninguna ley española

El Reglamento (UE) 2024/1689, conocido como AI Act, es de aplicación directa en toda la Unión Europea: obliga a las administraciones españolas igual que a las empresas, sin necesidad de transposición. Ha sido modificado por el Reglamento (UE) 2026/1744 (Ómnibus Digital de IA), en vigor desde el 27 de julio de 2026, que cambió varias fechas.

En el vocabulario del Reglamento, la administración que contrata y utiliza un sistema de IA es **responsable del despliegue**, y la empresa que lo desarrolla o lo comercializa con su nombre es el **proveedor**. Cada uno tiene obligaciones propias, y el pliego es el lugar donde se reparten y se hacen exigibles.

Desde	Qué se aplica	Por qué importa en una licitación
2 de febrero de 2025	Prácticas prohibidas (art. 5) y alfabetización en IA (art. 4)	Ningún pliego puede pedir un uso prohibido. El art. 4 establece que proveedores y responsables del despliegue «adoptarán medidas para apoyar la promoción de la alfabetización en materia de IA» de su personal: la formación de quien usará el sistema puede formar parte del objeto del contrato.
2 de agosto de 2025	Obligaciones de los modelos de IA de uso general y régimen sancionador del Reglamento	Conviene saber qué modelo de uso general hay debajo de la solución ofertada y quién lo suministra.
2 de agosto de 2026	Régimen general, incluidas las obligaciones de transparencia del art. 50 (con un periodo transitorio hasta el 2 de diciembre de 2026 para el marcado de contenidos generados, art. 50.2)	Un asistente de atención a la ciudadanía tiene que informar de que se está interactuando con un sistema de IA.
2 de diciembre de 2026	Dos prácticas prohibidas nuevas añadidas por el Ómnibus	Amplían la lista de usos que ningún contrato puede incluir.
2 de diciembre de 2027	Obligaciones de los sistemas de alto riesgo del anexo III	Muchos contratos que se firman hoy seguirán en ejecución en esa fecha.
2 de agosto de 2028	Alto riesgo en productos regulados (anexo I)	Afecta sobre todo a productos sanitarios, maquinaria y similares.
2 de agosto de 2030	Plazo máximo de adaptación (art. 111.2) para los sistemas de alto riesgo ya comercializados que usan autoridades públicas	Es más margen, no una exención.

Por qué el alto riesgo importa especialmente a las administraciones

El anexo III del Reglamento incluye ámbitos que son, en buena parte, actividad administrativa: el acceso a servicios y prestaciones públicas esenciales (evaluar si se tiene derecho a una prestación, concederla, reducirla o revocarla), el empleo y la selección de personal, la educación, la migración y el asilo, la administración de justicia o la aplicación de la ley. Un sistema que intervenga en esas decisiones será, con toda probabilidad, de alto riesgo.

Cuando lo es, la administración, como responsable del despliegue, asume obligaciones propias: utilizarlo conforme a sus instrucciones, encomendar la supervisión humana a personas con la competencia, la formación y la autoridad necesarias, conservar los registros que genera el sistema durante al menos seis meses e informar a las personas afectadas (art. 26). Las autoridades públicas, además, solo pueden utilizar sistemas de alto riesgo que estén registrados en la base de datos de la UE (art. 26.8) y, antes de ponerlos en servicio, deben hacer, salvo en el ámbito de las infraestructuras críticas, una evaluación de impacto sobre los derechos fundamentales (art. 27). Las personas afectadas por una decisión basada en un sistema de alto riesgo tienen derecho a una explicación (art. 86).

Nada de eso se puede cumplir si el proveedor no entrega la información necesaria, y por eso hay que pedirla en el pliego. Las obligaciones de alto riesgo se aplican desde el 2 de diciembre de 2027; para los sistemas de alto riesgo que ya estuvieran en el mercado y estén destinados a ser usados por autoridades públicas, el plazo máximo de adaptación es el 2 de agosto de 2030 (art. 111.2). Un contrato plurianual que se adjudique ahora tiene que prever ambas fechas.

En cuanto a las sanciones, el Reglamento fija multas de hasta 35 millones de euros o el 7 % del volumen de negocio para las prácticas prohibidas, y tramos inferiores para el resto. Si las autoridades públicas pueden ser multadas, y en qué medida, lo decide cada Estado miembro (art. 99.8). España todavía no lo ha concretado por ley.

La situación en España

El Proyecto de Ley Orgánica para el buen uso y la gobernanza de la inteligencia artificial, presentado en las Cortes el 28 de mayo de 2026, **decayó el 6 de octubre de 2026** con la disolución de las Cortes, antes de las elecciones generales del 29 de noviembre. Un nuevo Gobierno tendría que volver a aprobarlo y remitirlo. Mientras tanto, el Reglamento europeo se aplica igual; lo que sigue pendiente es la ley que concreta en España el régimen sancionador y el reparto de autoridades. La Agencia Española de Supervisión de la Inteligencia Artificial (AESIA), con sede en A Coruña, sigue existiendo.

Normativa conexa que entra en todo pliego con IA

Norma	Qué aporta al pliego
RGPD (Reglamento (UE) 2016/679)	Contrato de encargado del tratamiento (art. 28), transferencias internacionales (capítulo V), protección de datos desde el diseño (art. 25), seguridad del tratamiento (art. 32), evaluación de impacto (art. 35) y límites a las decisiones basadas únicamente en tratamientos automatizados (art. 22).
LOPDGDD (Ley Orgánica 3/2018)	Su disposición adicional primera obliga a aplicar a los tratamientos de datos del sector público las medidas de seguridad del Esquema Nacional de Seguridad.
Esquema Nacional de Seguridad (Real Decreto 311/2022)	Categorías básica, media y alta, y medidas de seguridad exigibles según la categoría. Se aplica también a los proveedores privados que prestan servicios o suministran soluciones al sector público.
Ley de Contratos del Sector Público (Ley 9/2017)	Cuando el contratista trata datos personales por cuenta de la administración, el pliego debe exigir una declaración sobre dónde estarán los servidores y desde dónde se prestarán los servicios, y la comunicación de cualquier cambio (art. 122.2). El cumplimiento de la normativa de protección de datos se incorpora como condición especial de ejecución (art. 202).
Ley 40/2015, de Régimen Jurídico del Sector Público	Para la actuación administrativa automatizada, exige designar previamente el órgano responsable de las especificaciones, la supervisión, el control de calidad y, en su caso, la auditoría del sistema y de su código fuente (art. 41).
Ley 15/2022, integral para la igualdad de trato	Pide a las administraciones favorecer que los algoritmos que intervienen en la toma de decisiones tengan en cuenta la minimización de sesgos, la transparencia y la rendición de cuentas (art. 23).

A esto se suma la normativa sectorial que corresponda (sanidad, educación, servicios sociales, tributos) y la de transparencia y acceso a la información pública. La IA no releva de ninguna de ellas.

01 Tratamiento exclusivo en el Espacio Económico Europeo

EL REQUISITO

Tratamiento exclusivo en el Espacio Económico Europeo, indicando regiones concretas y no solo el país de la sede del proveedor.

Qué exigir

- Que todo el tratamiento se realice dentro del EEE: almacenamiento, procesamiento, ejecución de los modelos de IA, copias de seguridad, registros de actividad y accesos de soporte técnico.
- Que el requisito alcance también al tránsito: ninguna petición puede enrutarse por servidores situados fuera del EEE, ni siquiera de forma ocasional por balanceo de carga, moderación de contenidos o telemetría.
- La identificación de las regiones o centros de datos concretos, no solo del país de la sede del licitador.
- La comunicación previa, y la autorización, de cualquier cambio de ubicación durante la ejecución.

Por qué

La sede del proveedor no dice nada sobre dónde se tratan los datos. Muchos servicios de IA procesan las peticiones en la región que tenga capacidad disponible en cada momento, y algunos componentes auxiliares pueden funcionar fuera de Europa aunque el almacenamiento principal esté aquí. Cualquier salida del EEE es una transferencia internacional sujeta al capítulo V del RGPD. Además, la Ley de Contratos del Sector Público ya obliga a que el pliego exija al adjudicatario declarar dónde estarán los servidores y desde dónde se prestarán los servicios asociados (art. 122.2). Este requisito convierte esa declaración en algo comprobable.

Cómo redactarlo en el pliego

CLÁUSULA TIPO

«El adjudicatario garantizará que todos los tratamientos de información derivados del contrato, incluidos el almacenamiento, el procesamiento, la ejecución de los modelos de IA, las copias de seguridad, los registros de actividad y los accesos de soporte, se realizan exclusivamente dentro del Espacio Económico Europeo, también en tránsito. Antes de la formalización presentará una declaración que identifique las regiones o centros de datos concretos y el lugar desde el que se prestarán los servicios asociados. Cualquier cambio de ubicación requerirá comunicación previa y autorización expresa del órgano de contratación.»

Dónde encaja. prescripciones técnicas y condición especial de ejecución (arts. 122.2 y 202 de la Ley 9/2017).

Qué evidencia pedir al licitador

- Declaración de ubicación de servidores y servicios, con las regiones identificadas.
- Documentación contractual del proveedor de nube y del proveedor del modelo que fije la región de tratamiento (el contrato, no la página comercial).
- Diagrama de flujos de datos, incluidos moderación, telemetría y soporte.
- Relación de subencargados con la ubicación de cada tratamiento.

02 Contrato de encargado del tratamiento

EL REQUISITO

Contrato de encargado del tratamiento conforme al artículo 28 del RGPD, con las garantías y los subencargados identificados.

Qué exigir

- Un contrato de encargo con el contenido mínimo del art. 28.3 del RGPD, firmado antes de que empiece cualquier tratamiento.
- La relación nominal de subencargados, incluidos el proveedor del modelo de IA y el de infraestructura, con su función y la ubicación del tratamiento.
- La autorización previa y por escrito para incorporar o sustituir subencargados (art. 28.2 del RGPD).
- La asistencia al responsable en evaluaciones de impacto, en el ejercicio de derechos y en la notificación de brechas, con un plazo de aviso concreto.
- El derecho de la administración a auditar o a recibir la información necesaria para comprobar el cumplimiento (art. 28.3.h del RGPD).

Por qué

Cuando el adjudicatario trata datos personales por cuenta de la administración es encargado del tratamiento, y el RGPD exige un contrato con un contenido mínimo. En los servicios de IA la cadena es larga: integrador, plataforma, proveedor del modelo, proveedor de nube. Cada eslabón es un subencargado, y si no está identificado la administración no sabe quién trata sus datos ni dónde. La propia Ley de Contratos del Sector Público obliga a que los licitadores indiquen en su oferta si van a subcontratar los servidores o los servicios asociados, con el nombre o el perfil empresarial de quien lo hará (art. 122.2).

Cómo redactarlo en el pliego

CLÁUSULA TIPO

«El adjudicatario tendrá la condición de encargado del tratamiento y suscribirá, antes del inicio de la ejecución, el contrato de encargo previsto en el artículo 28.3 del Reglamento (UE) 2016/679, que se incorpora como anexo a este pliego. En su oferta identificará todos los subencargados previstos, incluidos los proveedores de modelos de IA y de infraestructura, con indicación de su función y de la ubicación del tratamiento. La incorporación o sustitución de subencargados requerirá autorización previa y por escrito del responsable. El adjudicatario notificará cualquier violación de la seguridad de los datos en un plazo máximo de [24] horas desde que tenga conocimiento de ella.»

Dónde encaja. anexo al pliego de cláusulas administrativas y condición especial de ejecución.

Qué evidencia pedir al licitador

- Aceptación expresa del modelo de contrato de encargo anexo al pliego.
- Relación de subencargados con razón social, función y ubicación.
- Las condiciones de encargo que el licitador tiene firmadas con sus propios subencargados, en particular con el proveedor del modelo.
- Procedimiento de gestión y notificación de brechas de seguridad.

03 Compromiso de no entrenar modelos con la información

EL REQUISITO

Compromiso expreso de no utilizar la información para entrenar modelos, por contrato y no por política comercial.

Qué exigir

- La prohibición de usar cualquier información del contrato (consultas, documentos aportados, resultados y registros) para entrenar, reentrenar, ajustar o mejorar modelos de IA, propios o de terceros.
- Que la prohibición alcance a todos los subencargados, en especial al proveedor del modelo.
- La declaración de los plazos de conservación temporal que aplique cada componente del servicio (por ejemplo, para la vigilancia de usos abusivos) y del lugar donde se conserva esa información.
- Si la administración encarga un modelo ajustado con su propia información, que ese modelo sea de uso exclusivo de la administración y no se reutilice para otros clientes.

Por qué

Una política de uso publicada en una web puede cambiarse unilateralmente de un día para otro; una obligación contractual, no. Utilizar la información de la administración para entrenar modelos supone tratarla para una finalidad distinta de la contratada, lo que choca con el principio de limitación de la finalidad del RGPD (art. 5.1.b), y además expone información que puede ser reservada: un modelo entrenado con documentos puede llegar a reproducir fragmentos de ellos. Es también una manifestación concreta del deber de confidencialidad del contratista.

Cómo redactarlo en el pliego

CLÁUSULA TIPO

«El adjudicatario se obliga a no utilizar, ni permitir que sus subencargados utilicen, la información facilitada o generada en la ejecución del contrato, incluidas las consultas, los documentos, los resultados y los registros, para entrenar, reentrenar, ajustar o mejorar modelos de IA, ni para ningún fin distinto de la prestación contratada. Declarará los plazos y la ubicación de cualquier conservación temporal de dicha información en cada componente del servicio. Esta obligación tiene el carácter de obligación contractual esencial.»

Dónde encaja. condición especial de ejecución calificada como obligación esencial, de modo que su incumplimiento pueda ser causa de resolución.

Qué evidencia pedir al licitador

- La cláusula contractual o las condiciones de servicio empresariales del proveedor del modelo que excluyen el entrenamiento con datos del cliente (la versión contractual, no la política publicada).
- Declaración de plazos de conservación por componente.
- Descripción de la configuración aplicada (por ejemplo, desactivación de la conservación de historiales) y de cómo puede comprobarse.

04 Conformidad con el Esquema Nacional de Seguridad

> EL REQUISITO
>
> **Conformidad con el ENS** en la categoría que corresponda al sistema, con la declaración o certificación que proceda.

Qué exigir

- Que el pliego indique la categoría del sistema en el ENS (básica, media o alta). Determinarla es tarea de la administración y debe hacerse antes de licitar, porque condiciona qué proveedores y qué arquitecturas son viables.
- La acreditación de la conformidad en esa categoría: declaración de conformidad para la categoría básica y certificación de conformidad, emitida por una entidad de certificación acreditada, para las categorías media y alta.
- Que la acreditación cubra los servicios que realmente se utilizarán, incluidos los servicios en la nube y de IA de terceros, y que se mantenga vigente durante toda la ejecución.

Por qué

El Esquema Nacional de Seguridad (Real Decreto 311/2022) es obligatorio para los sistemas de información del sector público y se extiende a los proveedores privados que les prestan servicios o les suministran soluciones. La LOPDGDD, por su parte, obliga a aplicar sus medidas a los tratamientos de datos personales del sector público. Buena parte de las herramientas de IA diseñadas para la empresa privada no pueden sostener los requisitos de una categoría alta. Y hay un error frecuente: el licitador presenta un certificado del ENS vigente, pero su alcance no incluye el servicio concreto de IA o la región que se va a utilizar.

Cómo redactarlo en el pliego

> **CLÁUSULA TIPO**
>
> «El sistema objeto del contrato se ha categorizado como de categoría [BÁSICA / MEDIA / ALTA] conforme al Esquema Nacional de Seguridad, regulado por el Real Decreto 311/2022. El adjudicatario acreditará la conformidad con el ENS en dicha categoría de los sistemas y servicios que emplee en la ejecución, incluidos los servicios en la nube y de IA de terceros, mediante [declaración de conformidad / certificación de conformidad emitida por una entidad de certificación acreditada], y la mantendrá vigente durante toda la ejecución del contrato.»

Dónde encaja. solvencia técnica o prescripciones técnicas, según el procedimiento, y obligación durante la ejecución.

Qué evidencia pedir al licitador

- Declaración o certificado de conformidad vigente, con indicación expresa de su alcance.
- Documento que relacione los servicios ofertados con el alcance certificado de cada proveedor de la cadena.
- Datos de la entidad certificadora, para poder verificar el certificado.

05 Certificaciones de seguridad de la información

EL REQUISITO

Certificaciones de seguridad de la información del tipo ISO 27001, y de protección de datos en la nube del tipo ISO 27018.

Qué exigir

- Certificación ISO/IEC 27001 (sistema de gestión de la seguridad de la información) y, cuando haya datos personales en servicios en la nube, ISO/IEC 27018 (protección de datos personales en la nube pública).
- Certificados vigentes, emitidos por una entidad acreditada y con un alcance que comprenda los servicios ofertados.
- Decidir de antemano a quién se le exigen: al licitador, a los proveedores de infraestructura y de modelo que utilice, o a ambos. En contratos pequeños suele bastar con exigirlo a la infraestructura y pedir al licitador una descripción de sus propias medidas.
- La aceptación de certificados equivalentes y de otras pruebas de medidas equivalentes.

Por qué

Las certificaciones son una evidencia independiente, auditada por un tercero, de que existe un sistema de gestión de la seguridad y no solo buenas intenciones. Complementan al ENS, pero no lo sustituyen: el ENS es obligatorio en el sector público y una certificación ISO no exime de él. Como cualquier requisito de solvencia, deben ser proporcionadas al objeto del contrato y admitir equivalentes; de lo contrario, restringen la concurrencia sin añadir protección. La ISO/IEC 42001 (sistemas de gestión de la IA) es todavía reciente y poco extendida: hoy tiene más sentido valorarla como mérito que exigirla.

Cómo redactarlo en el pliego

CLÁUSULA TIPO

«El licitador acreditará que los servicios de infraestructura y de IA empleados en la ejecución cuentan con certificación vigente conforme a las normas ISO/IEC 27001 e ISO/IEC 27018, o equivalentes, emitida por entidad acreditada y cuyo alcance comprenda dichos servicios. Se admitirán otras pruebas de medidas equivalentes de gestión de la seguridad de la información.»

Dónde encaja. solvencia técnica; la ISO/IEC 42001, en su caso, como criterio de adjudicación.

Qué evidencia pedir al licitador

- Copia de los certificados, con alcance, fecha de emisión y vigencia.
- Identificación de la entidad certificadora y de su acreditación.
- Si el licitador no está certificado: descripción de las medidas equivalentes que aplica.

06 Trazabilidad completa

EL REQUISITO

Trazabilidad completa de accesos, consultas y resultados, con capacidad de reconstruir a posteriori qué ocurrió.

Qué exigir

- El registro automático de los accesos de usuarios, las entradas o consultas, la versión del modelo y de la configuración empleadas, los resultados generados y las intervenciones humanas de validación o corrección.
- Sello de tiempo y protección de los registros frente a alteraciones.
- Un plazo de conservación definido, que respete la normativa de protección de datos y, en sistemas de alto riesgo, el mínimo de seis meses que el Reglamento impone al responsable del despliegue (art. 26).
- Que la administración pueda consultar y exportar los registros por sí misma, en formato abierto, sin depender del proveedor y sin coste adicional.

Por qué

Meses después de una actuación, la administración puede tener que explicar en qué se basó: ante un recurso, una reclamación, una fiscalización o un incidente de seguridad. Si el sistema no deja rastro, esa explicación es imposible. El Reglamento de IA exige que los sistemas de alto riesgo permitan el registro automático de eventos (art. 12), el ENS exige registro de actividad y la Ley 40/2015 prevé la auditoría de los sistemas de actuación automatizada (art. 41). Una solución que no puede reconstruir cómo llegó a un resultado es inservible en lo público, por bien que funcione. Los registros contienen a su vez datos personales, por lo que hay que limitar su contenido y su plazo a lo necesario.

Cómo redactarlo en el pliego

CLÁUSULA TIPO

«El sistema registrará de forma automática, con sello de tiempo y protección frente a alteraciones, los accesos de usuarios, las entradas o consultas, la versión del modelo y de la configuración empleadas, los resultados generados y las intervenciones humanas de validación o corrección. Los registros se conservarán durante [plazo, no inferior a seis meses] y la Administración podrá consultarlos y exportarlos por sí misma en formato abierto y legible por máquina, sin coste adicional.»

Dónde encaja. prescripciones técnicas; la calidad de la solución de trazabilidad puede valorarse además como criterio de adjudicación.

Qué evidencia pedir al licitador

- Descripción del modelo de registro: campos, plazos de conservación, protección y control de acceso.
- Ejemplo de registro completo de una consulta de prueba.
- Demostración, en la fase de valoración o en un piloto, de la consulta y la exportación de registros.

07 Supervisión humana definida

EL REQUISITO

Supervisión humana definida en los puntos del proceso donde la decisión tiene consecuencias, especificando cuáles son.

Qué exigir

- Que el pliego identifique los puntos del proceso en los que una persona designada por la administración valida, corrige o descarta el resultado antes de que produzca efectos sobre personas o se incorpore a un acto administrativo.
- Que el sistema lo permita técnicamente: interfaz de revisión, posibilidad de modificar o descartar cada resultado y de detener el sistema.
- Que muestre la información necesaria para interpretar el resultado (fuentes consultadas, grado de confianza, limitaciones conocidas), para evitar la tendencia a dar por bueno lo que propone la máquina.
- Formación de las personas que ejercerán la supervisión.

Por qué

La IA puede preparar, ordenar y documentar el trabajo; no debe decidir por sí sola sobre las personas. El Reglamento de IA exige que los sistemas de alto riesgo se diseñen para permitir una supervisión humana efectiva (art. 14) y que el responsable del despliegue la encomiende a personas con la competencia, la formación y la autoridad necesarias (art. 26). El RGPD reconoce el derecho a no ser objeto de decisiones basadas únicamente en un tratamiento automatizado que produzcan efectos jurídicos (art. 22). Y una supervisión que no se ha definido de antemano acaba siendo, en la práctica, un clic de conformidad.

Cómo redactarlo en el pliego

CLÁUSULA TIPO

«El sistema no producirá efectos sobre personas ni se incorporará a actos administrativos sin la validación previa de una persona designada por la Administración en los siguientes puntos del proceso: [enumerarlos]. La interfaz permitirá revisar, modificar o descartar cada resultado, mostrará la información necesaria para interpretarlo y permitirá detener el sistema. El adjudicatario impartirá a las personas supervisoras la formación necesaria para ejercer esa función.»

Dónde encaja. prescripciones técnicas; la formación, como parte del objeto del contrato.

Qué evidencia pedir al licitador

- Descripción funcional del flujo de trabajo, con los puntos de intervención humana señalados.
- Capturas o demostración de la interfaz de revisión.
- Plan de formación de las personas supervisoras, que puede servir también como evidencia de alfabetización en IA (art. 4).

08 Descripción técnica, riesgos y clasificación

EL REQUISITO

Descripción técnica del sistema y gestión de riesgos documentadas, y clasificación razonada de si el sistema es o no de alto riesgo según el anexo III del Reglamento.

Qué exigir

- Una descripción técnica comprensible: finalidad, componentes, modelos (proveedor y versión), datos de entrada, métricas de error, limitaciones y condiciones de uso.
- Un plan de gestión de riesgos que cubra, como mínimo, errores, sesgos y discriminación, y seguridad, actualizado durante toda la ejecución.
- Una clasificación razonada conforme al Reglamento de IA: que no se trata de una práctica prohibida, si es o no de alto riesgo según el art. 6 y el anexo III, y qué obligaciones de transparencia del art. 50 le son aplicables.
- La información que la administración necesita como responsable del despliegue (instrucciones de uso, datos para la evaluación de impacto sobre los derechos fundamentales, registro en la base de datos de la UE) y, si el sistema es de alto riesgo, el compromiso de conformidad en las fechas de aplicación.

Por qué

Sin esta documentación la administración no puede cumplir sus propias obligaciones, y la clasificación determina todo lo demás. El Reglamento exige al proveedor que considere que un sistema del anexo III no es de alto riesgo que documente esa evaluación (art. 6.4); pedirla en el pliego obliga a hacer el análisis antes de adjudicar. La gestión de sesgos conecta con la Ley 15/2022 (art. 23). Y un contrato plurianual adjudicado hoy seguirá vivo el 2 de diciembre de 2027: debe dejar claro quién responde de la adaptación.

Cómo redactarlo en el pliego

CLÁUSULA TIPO

«El licitador aportará una descripción técnica del sistema y una clasificación razonada conforme al Reglamento (UE) 2024/1689, en la que justifique si el sistema es o no de alto riesgo según su artículo 6 y su anexo III y qué obligaciones de transparencia de su artículo 50 le resultan aplicables. Durante la ejecución mantendrá actualizado un plan de gestión de riesgos que incluya, como mínimo, los riesgos de error, de sesgo o discriminación y de seguridad, y facilitará a la Administración la información necesaria para cumplir sus obligaciones como responsable del despliegue. Si el sistema fuera de alto riesgo, garantizará su conformidad con el Reglamento en las fechas de aplicación previstas en él.»

Dónde encaja. documentación de la oferta (memoria técnica) y obligación durante la ejecución; la calidad del plan de riesgos puede ser criterio de adjudicación.

Qué evidencia pedir al licitador

- Memoria técnica y documento de clasificación conforme al Reglamento de IA, firmado por el licitador.
- Plan de gestión de riesgos con su procedimiento de actualización.
- Si es de alto riesgo: instrucciones de uso y calendario de conformidad.

09 Borrado verificable

EL REQUISITO

Borrado verificable de la información al terminar el contrato, con constancia de que se ha producido.

Qué exigir

- Al terminar el contrato, la devolución de toda la información tratada y generada, en formato abierto y estructurado.
- Su supresión posterior en todos los sistemas del adjudicatario y de sus subencargados, incluidos copias de seguridad, registros, historiales de conversación, índices de búsqueda, representaciones vectoriales y modelos ajustados con esa información.
- Un plazo concreto para cada paso, incluido el borrado de las copias de seguridad.
- Un certificado de borrado que identifique los sistemas afectados, el método y la fecha.

Por qué

El RGPD exige que el encargado suprima o devuelva los datos personales al terminar la prestación, a elección del responsable (art. 28.3.g). En los sistemas de IA la información persiste en lugares poco evidentes: los índices que permiten buscar en los documentos, las representaciones vectoriales, los historiales y los modelos ajustados. Si el pliego no lo concreta y no pide constancia, nadie lo comprobará.

Cómo redactarlo en el pliego

CLÁUSULA TIPO

«A la finalización del contrato, y en el plazo de [30] días, el adjudicatario devolverá a la Administración, en formato abierto y estructurado, toda la información tratada y generada durante su ejecución, y a continuación la suprimirá de todos sus sistemas y de los de sus subencargados, incluidas copias de seguridad, registros, historiales, índices de búsqueda, representaciones vectoriales y modelos ajustados con dicha información. Entregará un certificado de borrado que identifique los sistemas afectados, el método empleado y la fecha, sin perjuicio de la conservación que exija una norma legal.»

Dónde encaja. condición especial de ejecución y obligación de la fase de finalización; el contrato de encargo debe recogerlo igualmente.

Qué evidencia pedir al licitador

- Procedimiento de devolución y borrado, descrito en la oferta.
- Plazos de rotación y borrado de las copias de seguridad.
- Modelo del certificado de borrado que se entregará.
- Compromiso de los subencargados de aplicar el mismo procedimiento.

10 Propiedad del resultado y salida sin dependencias

EL REQUISITO

Propiedad del resultado y salida sin dependencias: código, documentación y configuración en poder de la administración, con traspaso previsto.

Qué exigir

- La titularidad de la administración sobre los desarrollos a medida: código fuente, configuraciones, instrucciones y flujos de trabajo del sistema, documentación y, en su caso, modelos ajustados con su información.
- La identificación de los componentes de terceros (modelos, plataformas, bibliotecas) con sus condiciones de licencia y su coste previsible tras el contrato.
- Un plan de traspaso que permita a la propia administración o a un tercero continuar el servicio: entrega completa, documentación suficiente y asistencia durante un periodo de transición.
- Una arquitectura que permita cambiar de proveedor de modelo sin rehacer la solución.

Por qué

Sin esto, al acabar el contrato la administración queda cautiva: la siguiente licitación tiene un único candidato realista y el coste de cambiar se convierte en el argumento para no hacerlo. En lo público hay además una razón de fondo: para la actuación administrativa automatizada, la Ley 40/2015 prevé la auditoría del sistema y de su código fuente (art. 41), y eso requiere tener acceso a él. Separar lo que es propio de lo que es de terceros permite saber de antemano qué se puede llevar la administración y qué tendrá que seguir licenciando.

Cómo redactarlo en el pliego

CLÁUSULA TIPO

«La Administración será titular de los derechos de explotación sobre los desarrollos realizados en ejecución del contrato, incluidos el código fuente, las configuraciones, las instrucciones y flujos de trabajo del sistema, la documentación y, en su caso, los modelos ajustados con su información. El licitador identificará en su oferta los componentes de terceros y sus condiciones de licencia. Antes de la finalización, el adjudicatario ejecutará un plan de traspaso que permita a la Administración o a un tercero continuar el servicio sin depender del adjudicatario, con entrega de toda la documentación y asistencia durante [plazo].»

Dónde encaja. pliego de cláusulas administrativas (propiedad intelectual) y prescripciones técnicas (plan de traspaso); la calidad del plan puede ser criterio de adjudicación.

Qué evidencia pedir al licitador

- Relación de componentes propios y de terceros, con sus licencias.
- Plan de traspaso o reversión, con calendario y entregables.
- Documentación de arquitectura que muestre cómo se sustituiría el modelo de IA.
- Demostración de la exportación de la configuración y los flujos.

Lista de comprobación para el pliego

Para marcar al redactar. Los números remiten a los requisitos de este documento.

Antes de redactar

- ☐ Está descrita la finalidad del sistema y los procesos concretos en los que se usará.
- ☐ Está determinada la categoría del sistema en el ENS (básica, media o alta).
- ☐ Se ha comprobado que el uso no es una práctica prohibida (art. 5) y se ha valorado si es de alto riesgo (anexo III).
- ☐ Se ha valorado la necesidad de una evaluación de impacto en protección de datos (art. 35 RGPD) y, si es alto riesgo, de la evaluación de impacto sobre los derechos fundamentales (art. 27 del Reglamento de IA).
- ☐ Se ha consultado a sistemas de información, a la persona delegada de protección de datos, a secretaría y a intervención.

Los diez requisitos

- ☐ **01** Tratamiento exclusivo en el EEE, con regiones concretas y declaración de ubicación de servidores.
- ☐ **02** Contrato de encargo conforme al art. 28 RGPD y subencargados identificados.
- ☐ **03** Prohibición contractual de entrenar modelos con la información, calificada como obligación esencial.
- ☐ **04** Categoría ENS indicada en el pliego y acreditación de conformidad con alcance suficiente.
- ☐ **05** ISO/IEC 27001 e ISO/IEC 27018, o equivalentes, con alcance que cubra los servicios.
- ☐ **06** Registro de accesos, consultas, resultados e intervenciones, exportable por la administración.
- ☐ **07** Puntos de supervisión humana enumerados y formación de las personas supervisoras.
- ☐ **08** Descripción técnica, plan de riesgos y clasificación razonada conforme al Reglamento de IA.
- ☐ **09** Devolución y borrado verificable, con certificado y plazo.
- ☐ **10** Titularidad de los desarrollos, licencias de terceros identificadas y plan de traspaso.

Al cerrar el pliego

- ☐ Los requisitos son proporcionados al objeto y al importe del contrato.
- ☐ Las certificaciones exigidas admiten equivalentes.
- ☐ La protección de datos figura como condición especial de ejecución (art. 202 LCSP).
- ☐ Están previstas consecuencias para el incumplimiento de los requisitos 01, 03 y 09.
- ☐ Está prevista la formación del personal que usará el sistema (art. 4 del Reglamento de IA).
- ☐ Si hay interacción con la ciudadanía, se exige el aviso de que se trata de un sistema de IA (art. 50).

Aviso y contacto

Aviso

Este documento tiene carácter informativo. No constituye asesoramiento jurídico ni sustituye el criterio de los servicios jurídicos, de la secretaría o de la intervención del órgano de contratación. Las cláusulas son modelos orientativos que deben adaptarse a cada expediente.

Refleja la normativa vigente en octubre de 2026, incluidos los cambios del Reglamento (UE) 2026/1744. El marco está en evolución, en Europa y en España: antes de utilizarlo conviene verificar la versión vigente de cada norma citada.

Puede reproducirse y adaptarse libremente en pliegos y expedientes, sin necesidad de autorización.

Sobre J2DIntelligence

J2DIntelligence es una consultora especializada en la adopción práctica de la inteligencia artificial, con una línea específica para el sector público: desarrollo de soluciones que nacen cumpliendo el ENS, la residencia de datos en el EEE y el Reglamento de IA; formación de empleados públicos en alfabetización en IA; y apoyo documental para pliegos y expedientes.

Soluciones de IA que cumplen la ley por diseño.

Si se está preparando un expediente, J2DIntelligence ofrece una primera reunión de media hora, sin compromiso, para revisar el planteamiento, la categoría del ENS aplicable y la viabilidad con las restricciones existentes, con un resumen por escrito que puede compartirse internamente.

> **Contacto**
>
> [correo de contacto] · [dominio definitivo]/sector-publico

J2DIntelligence es una marca comercial de Taller de Ideas para la Red, S.L. · NIF B04723896 · Calle San Pedro 11, 04001 Almería.