WHITE PAPER

SOBERANÍA DEL DATO

White Paper para la adopción responsable de Inteligencia Artificial
en Administraciones Públicas y empresas

Gobernanza · Confidencialidad · Trazabilidad · IA local

Javier Cabezas

Versión 1.5 | Edición Q4_2026
Documento marco de referencia

“La inteligencia artificial puede apoyar el trabajo. La organización conserva la responsabilidad de definir sus condiciones de uso, revisar sus resultados y responder por sus decisiones”.

Control de versiones

Versión	Fecha	Autor	Descripción	Validación
1.0	19/10/2026	Javier Cabezas	Versión editorial consolidada del cuerpo principal.	Pendiente
1.1	19/10/2026	Javier Cabezas	Incorporación de anexos operativos y caso práctico.	Pendiente
1.2	19/10/2026	Javier Cabezas	Regeneración íntegra con anexos y caso práctico.	Pendiente
1.3	19/10/2026	Javier Cabezas	Ampliación con casos prácticos de comunicación institucional y análisis de ofertas.	Pendiente
1.4	19/10/2026	Javier Cabezas	Revisión ortográfica, terminológica y de estilo formal.	Pendiente
1.5	11/11/2026	Javier Cabezas	Incorporación del marco normativo europeo 2018–2028 y referencias oficiales sobre soberanía cloud e IA.	Pendiente

Objeto del documento

El presente documento propone un marco práctico para la gestión de la información en las organizaciones que utilizan inteligencia artificial en sus procesos de trabajo.

Su finalidad consiste en facilitar la adopción de decisiones sobre qué información se utiliza, para qué tareas, en qué entornos, bajo qué condiciones y con qué revisión posterior.

La Soberanía del Dato se aborda como una capacidad organizativa: no depende de una herramienta concreta, sino de reglas claras, responsabilidades asignadas, controles proporcionales y evidencias conservadas.

«La inteligencia artificial puede apoyar el trabajo. La organización conserva la responsabilidad de definir sus condiciones de uso, revisar sus resultados y responder por sus decisiones».

Índice

Contenido principal

1. Resumen ejecutivo
2. Objeto y alcance
3. Principios básicos
4. Decálogo de la Soberanía del Dato
5. Método PROTEGE
6. Clasificación de la información
7. Gobernanza y responsabilidades
8. Relación con proveedores
9. Trazabilidad y evidencias
10. Ciclo de vida de la información
11. Gestión de incidentes
12. Implantación organizativa
13. Indicadores de seguimiento
14. Caso de aplicación: oferta técnica
15. Aplicación al proyecto Licitar y Ganar
16. Instrumentos de aplicación
17. Mantenimiento del marco
18. Criterios de éxito
19. Marco normativo europeo: del control del dato a la soberanía cloud e IA
20. Cierre

Anexos I-VIII: instrumentos y casos prácticos

Índice de anexos

Anexo	Título
I	Decálogo de la Soberanía del Dato
II	Matriz de clasificación de la información
III	Registro de uso de inteligencia artificial
IV	Modelo de acta de validación
V	Panel de indicadores
VI	Caso práctico 1: oferta técnica
VII	Caso práctico 2: comunicación institucional
VIII	Caso práctico 3: análisis y cotejo de ofertas

Siglas y abreviaturas

Sigla	Significado
IA	Inteligencia artificial
PROTEGE	Método de trabajo para la preparación de ofertas técnicas con apoyo de inteligencia artificial
RGPD	Reglamento General de Protección de Datos
AEPD	Agencia Española de Protección de Datos
ESPD	European Single Procurement Document

1. Resumen ejecutivo

La ***Soberanía del Dato*** constituye la capacidad de una organización para decidir, de forma consciente y documentada, cómo utiliza la información en sus procesos de trabajo.

En un entorno en el que la inteligencia artificial puede analizar, transformar y generar contenidos, esta capacidad resulta esencial para preservar la confidencialidad, la calidad, la trazabilidad y la responsabilidad sobre las decisiones adoptadas.

El documento establece principios, reglas de clasificación, fases de trabajo, mecanismos de gobernanza, controles relativos a los proveedores, procedimientos de gestión de incidentes, indicadores e instrumentos de implantación.

No se propone prohibir el uso de la inteligencia artificial, sino emplearla con criterio, reduciendo la exposición innecesaria de información y conservando el control humano sobre los resultados.

2. Objeto y alcance

El objeto del presente documento consiste en definir un marco común para decidir qué información puede utilizarse con inteligencia artificial, en qué condiciones, con qué finalidad y con qué controles posteriores.

Su ámbito de aplicación comprende las tareas de redacción, análisis documental, preparación de ofertas, gestión administrativa, comunicación institucional, análisis de datos y cualquier otra actividad en la que se utilice información organizativa.

Quedan fuera de su alcance las decisiones que corresponden exclusivamente a la representación legal de la organización, así como las obligaciones que se derivan de la normativa específica en materia de protección de datos, seguridad o contratación pública.

El marco deberá adaptarse a cada organización, manteniendo sus principios y ajustando los controles a su tamaño, actividad, sensibilidad de la información y recursos disponibles.

3. Principios básicos

Responsabilidad humana: la inteligencia artificial apoya el trabajo, pero las decisiones y los compromisos corresponden a personas identificables.

Confidencialidad: la información sensible no deberá compartirse más allá de lo estrictamente necesario.

Minimización: se utilizará la menor cantidad de información suficiente para realizar cada tarea.

Verificación: ningún resultado se incorporará automáticamente a un documento, expediente o comunicación.

Trazabilidad: deberá poder reconstruirse qué información se utilizó, qué herramienta se empleó, qué resultado se obtuvo y qué decisión se adoptó.

Proporcionalidad: los controles deberán ser adecuados al riesgo y no convertir el uso de la inteligencia artificial en una carga innecesaria.

Decisión explicable: la organización deberá poder explicar por qué aceptó, modificó o descartó un resultado.

4. Decálogo de la Soberanía del Dato

1. Definir qué información puede utilizarse antes de emplear cualquier herramienta.
2. Clasificar la información según su sensibilidad y su impacto potencial.
3. Utilizar la mínima información necesaria para cada tarea.
4. No introducir datos personales, secretos comerciales, credenciales ni documentación reservada sin una autorización expresa.
5. Conocer las condiciones del proveedor: tratamiento de los datos, conservación, entrenamiento de modelos y ubicación del servicio.
6. Revisar todo resultado antes de incorporarlo a un documento o comunicación.
7. Conservar las evidencias del uso realizado: instrucción, resultado, revisión y decisión.
8. Asignar responsabilidades claras a personas concretas.
9. Registrar y gestionar los incidentes de forma proporcionada.
10. Revisar periódicamente las reglas, las herramientas y los riesgos.

5. Método PROTEGE

El método PROTEGE estructura el uso de la inteligencia artificial en fases con entradas, salidas, responsables y controles definidos.

Fase 1. Preparar: identificar la tarea, la información necesaria, las restricciones y el resultado esperado.

Fase 2. Revisar: clasificar la información y determinar qué puede utilizarse, anonimizarse o excluirse.

Fase 3. Orientar: preparar instrucciones claras, con contexto suficiente y límites precisos.

Fase 4. Trabajar: utilizar la herramienta y obtener un resultado inicial.

Fase 5. Examinar: contrastar el resultado con las fuentes, los datos internos y los criterios de calidad.

Fase 6. Garantizar: validar el resultado desde las perspectivas técnica, económica, jurídica y organizativa.

Fase 7. Registrar: conservar las evidencias, las decisiones y las versiones definitivas.

Fase 8. Evaluar: aprender de los resultados, corregir las desviaciones y mejorar el procedimiento.

El método no concluye cuando la inteligencia artificial devuelve un texto. Concluye cuando el equipo conoce qué información utilizó, qué resultado aceptó, qué descartó, quién lo validó y qué ocurrió con la información posteriormente.

6. Clasificación de la información

La clasificación constituye el punto de partida para determinar el uso permitido de la información.

La información pública puede utilizarse con libertad, citando la fuente cuando proceda.

La información interna puede utilizarse en condiciones controladas, previa revisión de su sensibilidad.

La información confidencial requiere minimización, anonimización o exclusión, salvo autorización expresa.

La información especialmente protegida, incluidos los datos personales y la información reservada, no deberá introducirse en herramientas externas sin un análisis específico y una base jurídica o autorización adecuada.

7. Gobernanza y responsabilidades

Cada organización deberá designar responsables para la clasificación de la información, la autorización de uso, la revisión de resultados, la gestión de incidentes y el mantenimiento del marco.

La persona que utilice la herramienta responderá por la adecuación de la información introducida y por la revisión inicial del resultado.

La persona responsable de la materia responderá por la validación técnica o funcional del contenido.

La representación de la organización responderá por las decisiones que generen compromisos externos.

La gobernanza no deberá depender de una única persona: deberán existir suplencias, registros y procedimientos verificables.

8. Relación con proveedores

Antes de utilizar una herramienta externa, deberá conocerse quién trata los datos, con qué finalidad, durante qué período, en qué ubicación y con qué garantías.

Deberá comprobarse si los datos introducidos pueden utilizarse para entrenar modelos, si pueden ser revisados por personas, si se conservan tras la solicitud y si pueden eliminarse.

La elección del proveedor deberá documentarse, especialmente cuando vayan a tratarse categorías de información sensibles.

Los contratos o condiciones del servicio deberán revisarse periódicamente, dado que pueden modificarse sin que la organización tenga conocimiento inmediato.

9. Trazabilidad y evidencias

Toda utilización relevante de inteligencia artificial deberá dejar evidencia suficiente para reconstruir el proceso.

Como mínimo, deberán conservarse la finalidad, la herramienta utilizada, la información introducida, el resultado obtenido, las revisiones realizadas y la decisión final.

La trazabilidad no exige conservar toda la información de forma indiscriminada: deberá aplicarse un criterio de proporcionalidad y conservación definido por la organización.

Las evidencias permitirán responder ante auditorías, revisiones internas, incidentes o reclamaciones.

10. Ciclo de vida de la información

La Soberanía del Dato no se limita al momento de introducir información en una herramienta.

Comprende la creación, clasificación, uso, conservación, compartición, archivo y eliminación de la información.

El ciclo concluye cuando la organización decide y documenta qué debe ocurrir con cada dato.

La eliminación deberá ser verificable y respetar los plazos legales, contractuales y organizativos aplicables.

11. Gestión de incidentes

Se entenderá por incidente cualquier uso no autorizado, exposición indebida, error relevante, pérdida de control o resultado incorrecto que pueda afectar a la organización o a terceros.

Todo incidente deberá registrarse indicando la fecha, la descripción, la información afectada, las personas implicadas, las medidas adoptadas y el estado de resolución.

La respuesta deberá ser proporcional al riesgo: desde la corrección inmediata hasta la notificación a los responsables competentes.

Los incidentes deberán utilizarse como fuente de aprendizaje para mejorar las reglas, la formación y los controles.

12. Implantación organizativa

La implantación comenzará con la aprobación del marco, la designación de responsables y la comunicación interna de las reglas básicas.

Posteriormente deberán prepararse los instrumentos prácticos: matriz de clasificación, registro de uso, plantillas de revisión y procedimiento de gestión de incidentes.

La formación deberá centrarse en casos reales: qué información puede compartirse, cómo revisar un resultado y cómo documentar una decisión.

La implantación será progresiva y deberá iniciarse por los procesos de mayor impacto o mayor riesgo.

13. Indicadores de seguimiento

Los indicadores permitirán comprobar si el marco se aplica y si resulta útil.

Deberán medirse, entre otros, el número de usos registrados, el porcentaje de resultados revisados, los incidentes detectados, el tiempo de resolución y las mejoras incorporadas.

Los indicadores deberán revisarse periódicamente para evitar que se conviertan en un mero registro formal.

El objetivo no consiste en controlar por controlar, sino en mantener el uso de la inteligencia artificial dentro de condiciones seguras, útiles y responsables.

14. Caso de aplicación: oferta técnica

El caso de aplicación desarrolla la preparación de una oferta técnica para una licitación ficticia de mantenimiento de espacios públicos.

La empresa utiliza el método PROTEGE para analizar el pliego, clasificar la información, preparar instrucciones, revisar borradores, validar compromisos y documentar la autorización final.

El caso demuestra la capacidad de la empresa para distinguir las mejoras de redacción, los cambios de significado y los compromisos nuevos.

El caso tampoco demuestra que hayan desaparecido todos los riesgos. Demuestra cómo aplicar un procedimiento para compartir menos información, revisar lo recibido y conservar una decisión explicable.

«La mejora no consiste en que la inteligencia artificial redacte una oferta más ambiciosa, sino en que ayude a expresar con precisión una propuesta que la empresa conoce, puede justificar y está preparada para cumplir».

15. Aplicación al proyecto Licitar y Ganar

Licitar y Ganar aplica estos principios a la preparación de ofertas y a la gestión de la información en los procesos de contratación.

El proyecto parte de una idea sencilla: la inteligencia artificial puede ayudar a redactar, analizar y organizar, pero la empresa deberá decidir qué ofrece, comprobar que puede cumplirlo y responder por lo que presenta.

La Soberanía del Dato se convierte así en un criterio de calidad y de confianza, no en una limitación artificial del uso de la tecnología.

16. Instrumentos de aplicación

Matriz de clasificación de la información.

Registro de uso de inteligencia artificial.

Plantilla de instrucciones o prompts.

Lista de comprobación para la revisión de resultados.

Acta de validación y autorización.

Registro de incidentes.

Panel de indicadores.

Guía breve de formación para las personas usuarias.

17. Mantenimiento del marco

El marco deberá revisarse al menos una vez al año y siempre que se incorpore una nueva herramienta, se modifique un proveedor o se detecte un incidente relevante.

Las revisiones deberán documentarse en el control de versiones.

Las reglas obsoletas deberán retirarse y las nuevas deberán comunicarse con claridad.

El mantenimiento constituye una responsabilidad continua, no un acto puntual.

18. Criterios de éxito

Las personas conocen qué información pueden utilizar y qué información debe protegerse.

Los resultados de la inteligencia artificial se revisan antes de su utilización.

Las decisiones relevantes quedan documentadas y son explicables.

Los incidentes se detectan, se gestionan y permiten aprender.

La organización mantiene el control sobre sus procesos sin renunciar a las ventajas de la tecnología.

19. Marco normativo europeo: del control del dato a la soberanía cloud e IA

La Soberanía del Dato no constituye hoy una obligación jurídica única y autónoma formulada con ese nombre. Sin embargo, el Derecho de la Unión ya exige un conjunto creciente de obligaciones de control, minimización, seguridad, trazabilidad, portabilidad, continuidad, supervisión humana y gestión de proveedores. En función del riesgo y de la sensibilidad de la información, una arquitectura local o soberana puede ser una medida técnica y organizativa especialmente adecuada para demostrar ese control.

La conclusión jurídica correcta no es “Europa obliga a instalar un servidor local”. La conclusión es: “Europa obliga a demostrar control; la infraestructura local o soberana puede ser una respuesta proporcionada cuando reduce de forma verificable la exposición, la dependencia o el riesgo”.

19.1. Obligaciones y marcos ya aplicables

Norma	Situación	Qué exige o regula	Lectura para Soberanía del Dato
RGPD	Aplicable	Responsabilidad demostrable; protección desde el diseño y por defecto; minimización; seguridad; EIPD cuando exista alto riesgo; reglas de transferencias internacionales.	Obliga a conocer y controlar tratamiento, accesos, encargados y riesgos. La localización puede ser una medida adecuada, no una obligación general.
Data Governance Act	Aplicable desde 24/09/2023	Para determinadas categorías de datos protegidos del sector público permite exigir reutilización remota dentro de un entorno de tratamiento seguro facilitado o controlado por el organismo público.	Da respaldo normativo al patrón “llevar el procesamiento al dato” cuando la sensibilidad lo aconseja.
Data Act	Aplicable desde 12/09/2025	Obliga a facilitar el cambio entre servicios de tratamiento de datos, incluso hacia infraestructura TIC on-premises; protege datos no personales de la UE frente a accesos públicos de terceros países incompatibles con el	Reduce lock-in y reconoce expresamente la infraestructura propia como destino de portabilidad. Cargos de cambio eliminados desde 12/01/2027.

		Derecho de la Unión.	
AI Act	Aplicación progresiva	Alfabetización en IA desde 02/02/2025; gran parte del Reglamento y supervisión desde 02/08/2026; transparencia; gobernanza; obligaciones reforzadas para alto riesgo.	Exige gobernar quién usa IA, para qué y con qué supervisión. Alto riesgo: 02/12/2027; IA de alto riesgo integrada en productos: 02/08/2028.
NIS2	Directiva; concreción nacional	Gestión de riesgos, incidentes, continuidad, backups, cadena de suministro, vulnerabilidades, criptografía, control de accesos y formación.	Refuerza segmentación, mínimo privilegio, continuidad y control de proveedores. La aplicación concreta a una entidad local depende de la transposición nacional.
Cyber Resilience Act	Aplicación parcial 2026; general 11/12/2027	Requisitos de ciberseguridad durante el ciclo de vida de productos con elementos digitales; notificación de vulnerabilidades/incidentes desde 11/09/2026.	Debe incorporarse progresivamente a criterios de compra, actualización y mantenimiento de software/appliances de IA.
Interoperable Europe Act	Aplicable; ámbito específico	Interoperabilidad de servicios públicos digitales transeuropeos; evaluaciones desde 12/01/2025; prioridad a soluciones sin licencias restrictivas cuando sean equivalentes.	Apoya estándares abiertos, APIs interoperables y menor dependencia tecnológica en su ámbito.
CADA	PROPUESTA · procedimiento en curso	COM(2026) 502 propone un marco europeo de soberanía cloud e IA y cuatro niveles de garantía para uso por organismos públicos según su evaluación de riesgos.	No es obligación vigente. Es la señal legislativa más explícita de la dirección europea hacia autonomía, control jurisdiccional y resiliencia cloud/IA.

19.2. Tres piezas especialmente relevantes

Data Governance Act. El artículo 5 permite que determinadas categorías de datos protegidos del sector público se reutilicen a distancia dentro de un entorno de tratamiento seguro facilitado o controlado por el organismo público, e incluso físicamente en instalaciones seguras cuando el acceso remoto ponga en peligro derechos o intereses de terceros. Este patrón normativo respalda la idea de acercar el procesamiento al dato.

Data Act. El Reglamento reconoce expresamente el cambio desde servicios cloud hacia infraestructura TIC on-premises y obliga a eliminar obstáculos técnicos, contractuales y organizativos al cambio. Además, su artículo 32 exige medidas para impedir accesos o transferencias de datos no personales almacenados en la Unión por autoridades de terceros países cuando entren en conflicto con el Derecho europeo o nacional.

AI Act. Desde el 2 de agosto de 2026 son aplicables la mayoría de sus reglas y la supervisión de las obligaciones ya vigentes. La alfabetización en IA se exige desde el 2 de febrero de 2025. Las reglas reforzadas para determinados sistemas de alto riesgo tienen un calendario posterior. La consecuencia organizativa es clara: utilizar IA exige gobierno, formación, supervisión y trazabilidad, no solo disponer de una herramienta.

19.3. CADA: la soberanía cloud e IA entra explícitamente en la agenda legislativa

El 3 de junio de 2026 la Comisión presentó COM(2026) 502, propuesta de Cloud and AI Development Act (CADA). A 11 de noviembre de 2026 el procedimiento legislativo ordinario 2026/0138/COD continúa en curso. Por tanto, no es todavía Derecho aplicable y debe citarse siempre como propuesta.

La propuesta es especialmente relevante porque define un marco europeo de soberanía en la nube y la IA con cuatro niveles de garantía destinados a ser utilizados por organismos del sector público en función de su evaluación de riesgos: desde tratamiento y almacenamiento en infraestructura situada en la Unión hasta niveles reforzados de independencia de terceros países, control europeo y transparencia de la cadena de software.

Su valor para este White Paper es prospectivo: confirma que autonomía, jurisdicción, cadena de suministro, resiliencia y control de la infraestructura cloud/IA han pasado a formar parte explícita de la agenda legislativa europea.

19.4. Línea temporal europea 2018–2028

Fecha	Norma / iniciativa	Hito
2018	RGPD	Control, privacidad desde diseño, seguridad y transferencias.
24/09/2023	Data Governance Act	Entornos de tratamiento seguros controlados por el sector público.
12/07/2024 / 12/01/2025	Interoperable Europe Act	Interoperabilidad pública; evaluaciones en su ámbito.
02/02/2025	AI Act	Prohibiciones iniciales y alfabetización en IA.
12/09/2025	Data Act	Portabilidad cloud/on-prem y control de accesos extraterritoriales.
02/08/2026	AI Act	Aplicación de la mayoría de reglas y supervisión.
11/09/2026	Cyber Resilience Act	Comienzan obligaciones de notificación del art. 14.
03/06/2026	CADA	Propuesta europea de soberanía cloud e IA; procedimiento legislativo en curso.
12/01/2027	Data Act	Eliminación de cargos de cambio/salida en los términos del Reglamento.
02/12/2027	AI Act	Sistemas independientes de IA de alto riesgo.
11/12/2027	Cyber Resilience Act	Aplicación general.
02/08/2028	AI Act	Sistemas de alto riesgo integrados en productos.

19.5. Criterio de aplicación

La decisión entre cloud, entorno europeo, infraestructura privada o IA local debe documentarse mediante una evaluación de riesgos y de la información tratada. Cuanto mayor sea la sensibilidad, el impacto de una indisponibilidad, la dependencia del proveedor, la exposición jurisdiccional o la

necesidad de confidencialidad, mayor es la justificación para incrementar el nivel de soberanía técnica.

En este marco, “IA soberana” no debe utilizarse como sinónimo de aislamiento absoluto. Significa conservar capacidad efectiva de decisión sobre datos, modelos, infraestructura, proveedores, accesos, evidencias y continuidad.

Fuentes oficiales de la Unión Europea

RGPD · Reglamento (UE) 2016/679

Data Governance Act · Reglamento (UE) 2022/868

Data Act · Reglamento (UE) 2023/2854

AI Act · Reglamento (UE) 2024/1689

Comisión Europea · calendario y aplicación del AI Act

NIS2 · Directiva (UE) 2022/2555

Cyber Resilience Act · Reglamento (UE) 2024/2847

Interoperable Europe Act · Reglamento (UE) 2024/903

CADA · Propuesta COM(2026) 502

CADA · estado del procedimiento 2026/0138/COD

Comisión Europea · soberanía tecnológica

Comisión Europea · Data Union Strategy

20. Cierre

La Soberanía del Dato no consiste en frenar la innovación, sino en utilizarla con control, criterio y responsabilidad.

Una organización con soberanía sobre sus datos conoce qué información utiliza, para qué, con quién, bajo qué condiciones y con qué consecuencias.

La inteligencia artificial puede mejorar la productividad y la calidad del trabajo, pero la confianza se construye mediante reglas claras, revisión humana y trazabilidad.

Anexo I. Decálogo de la Soberanía del Dato

N.º	Regla	Aplicación práctica
1	Definir qué información puede utilizarse antes de emplear cualquier herramienta.	[Describir su aplicación en la organización]
2	Clasificar la información según su sensibilidad.	[Describir su aplicación en la organización]
3	Utilizar la mínima información necesaria.	[Describir su aplicación en la organización]
4	No introducir datos personales, secretos comerciales, credenciales ni documentación reservada sin autorización expresa.	[Describir su aplicación en la organización]
5	Conocer las condiciones del proveedor.	[Describir su aplicación en la organización]
6	Revisar todo resultado antes de incorporarlo.	[Describir su aplicación en la organización]
7	Conservar las evidencias del uso.	[Describir su aplicación en la organización]
8	Asignar responsabilidades claras.	[Describir su aplicación en la organización]
9	Registrar y gestionar los incidentes.	[Describir su aplicación en la organización]
10	Revisar periódicamente las reglas, las herramientas y los riesgos.	[Describir su aplicación en la organización]

Anexo II. Matriz de clasificación de la información

Nivel	Ejemplos	Uso con inteligencia artificial	Controles
Pública	Pliegos, normativa, publicaciones	Permitido	Citar la fuente cuando proceda
Interna	Procedimientos, plantillas, documentación de trabajo	Condicional	Revisión previa y minimización
Confidencial	Precios, márgenes, estrategias, datos de clientes	Restringido	Anonimización o autorización expresa
Especialmente protegida	Datos personales, información reservada, credenciales	Prohibido por defecto	Análisis específico y base jurídica o autorización

Anexo III. Registro de uso de inteligencia artificial

Fecha	Persona usuaria	Herramienta	Finalidad	Información introducida	Resultado	Revisión	Decisión
[Fecha]	[Nombre]	[Herramienta]	[Finalidad]	[Descripción]	[Resumen o referencia]	[Revisor]	[Aceptado, modificado o descartado]

Anexo IV. Modelo de acta de validación

Se hace constar que el documento o resultado indicado ha sido revisado y validado conforme al marco de Soberanía del Dato.

Elemento	Contenido
Documento o resultado	[Identificación]
Fecha de revisión	[Fecha]
Personas participantes	[Nombres y funciones]
Comprobaciones realizadas	[Detalle]
Reservas o incidencias	[Detalle]
Decisión	[Aprobado, aprobado con reservas o rechazado]
Firma	_____

Anexo V. Panel de indicadores

Indicador	Fórmula	Frecuencia	Responsable
Usos registrados	Número de registros del período	Mensual	Responsable del seguimiento
Resultados revisados	Resultados revisados / resultados generados	Mensual	Responsable de la revisión
Incidentes	Número de incidentes del período	Mensual	Responsable de los incidentes
Tiempo de resolución	Media de días entre la detección y el cierre	Mensual	Responsable de los incidentes
Mejoras implantadas	Número de mejoras incorporadas	Trimestral	Responsable del marco

Anexo VI. Caso práctico 1: oferta técnica

El presente caso desarrolla, de principio a fin, la aplicación del método PROTEGE a una oferta técnica para una licitación ficticia de mantenimiento de espacios públicos.

VI.1. Presentación del caso

Una pequeña empresa prepara una oferta para una licitación de mantenimiento de espacios públicos. El caso muestra cómo aplicar un procedimiento para compartir menos información, revisar lo recibido y conservar una decisión explicable.

La documentación de trabajo incluye los pliegos y la documentación publicada de la convocatoria, la memoria técnica en preparación, el presupuesto y los cálculos internos de rentabilidad.

VI.2. Desarrollo fase a fase

Fase 1. Análisis del pliego: identificación de los requisitos obligatorios, criterios de adjudicación, plazos, garantías y condiciones de ejecución.

Fase 2. Clasificación de la información: determinación de los datos utilizables, anonimizables o excluidos.

Fase 3. Preparación de instrucciones: redacción de instrucciones concretas, con contexto suficiente y límites claros.

Fase 4. Generación y revisión de borradores: revisión, corrección y adaptación de los textos propuestos.

Fase 5. Contraste con la documentación interna: comprobación de la capacidad real de la empresa.

Fase 6. Validación técnica, económica y jurídica.

Fase 7. Aprobación, registro y conservación de las evidencias.

Fase 8. Seguimiento posterior y lecciones aprendidas.

VI.3. Revisión final y autorización

Se comprobará la coherencia entre la memoria técnica, el presupuesto, los medios asignados y los compromisos asumidos.

La oferta podrá considerarse preparada cuando existan evidencias de la revisión técnica, económica y jurídica, así como de la conformidad de la representación de la empresa.

VI.4. Anexos del caso

Anexo	Contenido
I	Documentación de trabajo utilizada
II	Matriz de requisitos del pliego
III	Clasificación de la información
IV	Instrucciones o prompts utilizados

Anexo	Contenido
V	Registro de revisiones
VI	Acta de validación y autorización
VII	Ficha de lecciones aprendidas
VIII	Cálculos económicos y de rentabilidad

VI.5. Cálculos económicos

Coste total de personal = Σ (Horas estimadas × Coste por hora)

Coste directo + Costes indirectos + Garantías y seguros + Margen comercial = Base imponible

Base imponible + IVA = Precio de licitación, cuando proceda

Punto de equilibrio = Costes fijos / (Precio unitario − Coste variable unitario)

Bloque	Contenido por completar
Supuestos	Duración, horas, coste por hora, costes indirectos y margen
Personal	Categorías, horas, coste por hora y total
Materiales y estructura	Bases, coeficientes e importes
Precio	Coste directo, costes indirectos, garantías, margen, base imponible, IVA y precio
Escenarios	Optimista, base y pesimista
Punto de equilibrio	Costes fijos, precio unitario, coste variable unitario y resultado

Anexo VII. Caso práctico 2: comunicación institucional

Un servicio municipal debe preparar una nota informativa sobre una nueva línea de ayudas al comercio local. El equipo utiliza inteligencia artificial para mejorar la claridad y la estructura del texto, sin incorporar datos personales de solicitantes ni información reservada.

VII.1. Punto de partida

Se dispone de la resolución de la convocatoria, de las bases reguladoras, de los datos públicos de la ayuda y de un borrador interno de comunicación.

La información relativa a identidades, importes individualizados y situaciones personales queda excluida del uso con herramientas externas.

VII.2. Aplicación del método

Preparar: definir el destinatario, el mensaje principal y el canal de difusión.

Revisar: eliminar los datos personales y comprobar la naturaleza pública de la información.

Orientar: solicitar un texto claro, accesible y neutro, sin compromisos no previstos.

Trabajar: obtener una propuesta de redacción.

Examinar: contrastar importes, plazos, requisitos y condiciones con las bases reguladoras.

Garantizar: validación técnica y jurídica antes de la publicación.

Registrar: conservar la instrucción, el resultado, la revisión y la versión aprobada.

Evaluar: recoger las incidencias y mejorar la plantilla.

VII.3. Control de calidad

Comprobación	Criterio	Resultado
Datos personales	No se incluyen datos identificativos	[Conforme o no conforme]
Exactitud	Los importes, plazos y requisitos coinciden con las bases	[Conforme o no conforme]
Tono institucional	Lenguaje claro, neutro y accesible	[Conforme o no conforme]
Compromisos	No se generan obligaciones no previstas	[Conforme o no conforme]
Autorización	Validación por el responsable competente	[Conforme o no conforme]

VII.4. Resultado esperado

Una comunicación institucional clara, verificable y publicable, con trazabilidad del uso de la inteligencia artificial y sin exposición de información protegida.

Anexo VIII. Caso práctico 3: análisis y cotejo de ofertas

Un órgano de contratación debe analizar varias ofertas presentadas en un procedimiento de servicios. La inteligencia artificial se utiliza para organizar la información y detectar posibles omisiones, sin sustituir la valoración ni la decisión del órgano competente.

VIII.1. Punto de partida

Se dispone de las ofertas presentadas, de la documentación administrativa y técnica, de los criterios de valoración y de las actas de la mesa de contratación.

Los documentos que contengan datos personales, secretos empresariales o información reservada se anonimizarán o se trabajarán mediante extractos no identificativos.

VIII.2. Aplicación del método

Preparar: definir los criterios de valoración y la documentación exigida.

Revisar: anonimizar las ofertas y excluir la información protegida.

Orientar: solicitar una tabla comparativa por criterios, sin valoración final.

Trabajar: obtener un cuadro de coincidencias, omisiones y diferencias.

Examinar: contrastar cada resultado con la oferta original.

Garantizar: validación por la mesa o el órgano competente.

Registrar: conservar la matriz, las revisiones y el acta.

Evaluar: incorporar mejoras al procedimiento de análisis.

VIII.3. Matriz comparativa

Criterio	Oferta A	Oferta B	Oferta C	Observaciones
Administrativa	[Cumple o no cumple]	[Cumple o no cumple]	[Cumple o no cumple]	[Observación]
Técnica	[Valoración]	[Valoración]	[Valoración]	[Observación]
Económica	[Importe]	[Importe]	[Importe]	[Observación]
Documentación	[Completa o incompleta]	[Completa o incompleta]	[Completa o incompleta]	[Observación]

VIII.4. Límites

La inteligencia artificial no valora ni adjudica. Su resultado constituye un apoyo para la organización y la detección de incidencias, siempre sujeto a revisión humana y a las reglas del procedimiento.

La decisión corresponde exclusivamente al órgano competente, conforme a los criterios publicados y a la documentación obrante en el expediente.

Cierre

La presente versión incorpora el cuerpo principal consolidado, los anexos operativos y tres casos prácticos completos: preparación de una oferta técnica, comunicación institucional y análisis y cotejo de ofertas.

Los campos entre corchetes deberán completarse con los datos y las evidencias definitivas.

Última revisión: 11 de noviembre de 2026.

Responsable: Javier Cabezas.