

FUNDADOR SUPREMO

LA PÁGINA POR HERRAMIENTA

Propuesta de complemento operativo a las orientaciones de la Agencia Española de Protección de Datos sobre inteligencia artificial agéntica y protección de datos

Documento de referencia: «Inteligencia Artificial Agéntica desde la Perspectiva de Protección de Datos», versión 1.2, febrero de 2026, 76 páginas, de la Agencia Española de Protección de Datos.

Disponible en: www.aepd.es/guias/orientaciones-ia-agentica.pdf

Propuesta abierta dirigida a la Agencia Española de Protección de Datos
y a cualquier responsable o encargado de tratamiento que despliegue agentes de IA.

Kenyi Martín Alcántara

Editor de fundadorsupremo.org · Asesor fiscal y jurídico de empresas · Perito judicial

Madrid, 26 de septiembre de 2026

Nota de identidad. Este es un documento de propuesta independiente, de carácter editorial y divulgativo. No ha sido emitido, encargado ni avalado por la Agencia Española de Protección de Datos, y no debe presentarse como material de la Agencia. Su autor no forma parte de ningún organismo público. Las referencias a las orientaciones oficiales se citan expresamente como ajenas.

· ÍNDICE

I.	Objeto de la propuesta
II.	Punto de partida: lo que las orientaciones ya aportan
III.	El hueco operativo: de la medida al formato
IV.	La propuesta: una página por herramienta de uso real
V.	Contenido de la página: siete bloques
VI.	Correspondencia con las medidas de la guía
VII.	Modo de empleo mínimo
VIII.	Límites de esta propuesta
Anexo A.	Plantilla en blanco de la página por herramienta

I. OBJETO DE LA PROPUESTA

Las orientaciones de la Agencia Española de Protección de Datos sobre IA agéntica [AEPD 2026] enumeran, en su capítulo VII, un conjunto amplio de medidas que un responsable o encargado puede adoptar: gobernanza, evaluación continua basada en evidencias, minimización, control de la memoria, puntos de intervención humana, cortacircuitos o trazabilidad, entre otras. El documento, como él mismo advierte, es un estudio introductorio que no analiza tratamientos concretos.

Esta propuesta no discute ninguna de esas medidas. Las acepta y parte de ellas. Lo que propone es un paso más pequeño y más operativo: convertir ese repertorio en un único instrumento de una página por herramienta, con campos concretos, que el responsable pueda rellenar, fechar y mostrar. La llamamos, provisionalmente, la página por herramienta.

La sugerencia a la Agencia es doble. Que valore si un formato de este tipo, depurado con su criterio, merece incorporarse como anexo a las orientaciones, cuyo capítulo de medidas enumera medidas y trata la documentación, pero no ofrece una plantilla única de una página por herramienta para reunir estos controles. Y que valore si ese formato puede servir de pieza de enlace entre las orientaciones y el registro de actividades de tratamiento, de modo que el responsable que rellena la página quede a un paso de actualizar su registro, y no a diez.

II. PUNTO DE PARTIDA: LO QUE LAS ORIENTACIONES YA APORTAN

Cuatro piezas de la guía sirven de cimiento directo a esta propuesta, y conviene dejarlas citadas antes de construir nada encima.

La regla de 2

En el capítulo de gestión del riesgo, la guía adapta una regla de seguridad para aplicaciones en navegadores y la plantea como umbral mínimo que no debiera traspasarse [cap. VG, fig. 13]. Tres circunstancias no deberían concurrir a la vez. Que el agente trate automáticamente información no controlada, que acceda a información sensible y que ejecute acciones automáticas. De las tres, como mucho dos, y cada combinación admisible exige su contrapartida; la que junta lectura sin control y acción automática obliga a impedir el acceso a información sensible o a datos personales. El ejemplo de la propia guía es un agente que responde correos. Las tres preguntas se hacen en una conversación; verificar las garantías que cubren cada pareja exige después comprobar el diseño y los controles efectivos del agente.

La memoria por defecto, como cosa a evitar

Al tratar la protección de datos desde el diseño y por defecto, la guía pide evitar la «memoria por defecto» de datos innecesarios y de registros de actividad incontrolados [cap. VH]. Y distingue, en el capítulo de vulnerabilidades, dos memorias. La de trabajo, que sirve para funcionar, y la de gestión, formada por los registros de todo lo que el sistema hizo [cap. IV.C]. Ambas pueden acumular copias sin plazo decidido por nadie.

Las condiciones de la supervisión humana efectiva

La guía no se limita a pedir supervisión. Aconseja ponderar varios criterios al evaluar si la intervención humana es efectiva. Competencia y autoridad para alterar el resultado. Preparación para evaluar la decisión. Independencia frente a presiones. Diligencia frente al sesgo de automatización. Y medios, esto es, procedimientos, información, recursos y tiempo [cap. VII.E]. Una supervisión sin autoridad, preparación o medios suficientes puede resultar ineficaz, y la guía advierte además contra desplazar al supervisor la responsabilidad que corresponde al diseño del tratamiento [cap. VI.A].

Los controles con nombre

El capítulo VII nombra piezas concretas: catálogos y listas blancas de servicios, puntos de aprobación humana que pueden incluir acciones irreversibles, reversibilidad de acciones, rutas de escalamiento, cortacircuitos que interrumpen bucles y accesos masivos, política selectiva de no registro, plazos de retención estrictos y trazabilidad del ciclo de vida del dato [cap. VII].

LO QUE NO HACE ESTA PROPUESTA

No reformula ninguna medida de la guía, no corrige ninguna definición y no añade doctrina propia sobre el RGPD. Toma el repertorio del capítulo VII y le busca un soporte de una página. Si la Agencia entendiera que el formato induce a error en algún punto, el formato se corrige; el repertorio sigue siendo suyo.

III. EL HUECO OPERATIVO: DE LA MEDIDA AL FORMATO

Una enumeración de medidas responde a la pregunta «¿qué debería existir?». El responsable de un despacho mediano, con tres herramientas de IA en uso real y una cuarta que alguien probó una tarde, se enfrenta a otra pregunta, la de dónde escribe lo que ya tiene. Esa distancia entre el repertorio y el papel es donde se pierden los cumplimientos.

La propia guía apunta en esta dirección sin llegar al formato. Pide gobernanza y la llama la medida más importante [cap. VII.A]. Pide aceptar la posibilidad de fallo y documentar decisiones, arquitectura y evolución [cap. VII.A y VII.F]. Pide actualizar el registro de actividades cuando el tratamiento cambia de medios [cap. VD]. Pero entre la medida y el registro no hay pieza intermedia: no existe en el documento un formato mínimo donde el responsable anote, herramienta por herramienta, qué lee, qué recuerda y qué puede ejecutar sola.

La plantilla pretende evitar que la información sobre cada herramienta quede dispersa entre documentos o sin campos comunes. Un formato canónico, aunque fuera orientativo, tendría tres virtudes: convertiría una lista de intenciones en un documento fechado; haría comparable el estado de dos organizaciones, o de la misma organización en dos momentos; y daría al proveedor un cuestionario estable al que responder, en lugar de que cada cliente invente el suyo.

IV. LA PROPUESTA: UNA PÁGINA POR HERRAMIENTA DE USO REAL

La página por herramienta es exactamente eso. Una página, por cada herramienta de IA con agentes que la organización use de verdad. No por cada herramienta probada. No por cada versión. Una página que cabe en una hoja, pensada para rellenarse en una sola sentada la primera vez y revisarse cuando cambia algo.

Tres principios la gobiernan, tomados del espíritu de la propia guía:

- Uso real, no catálogo de intenciones. La página se escribe para las herramientas que tocan datos del negocio, no para las que aparecen en la última feria. Si la herramienta se retira, la página se archiva, no se borra: lo retirado también es expediente.
- Fecha y firma. Cada página lleva fecha de edición y responsable. Un inventario sin fecha no demuestra nada, y la guía pide evidencia de cumplimiento, no de buenas intenciones [cap. VII.B].
- Revisión por acontecimiento. La página se revisa cuando cambia la herramienta, sus términos, su versión o su alcance de permisos, sin sustituir la monitorización y la evaluación continuas que procedan. La guía ya exige control sobre las actualizaciones [cap. VII.F]; la página es donde ese control deja rastro.

V. CONTENIDO DE LA PÁGINA: SIETE BLOQUES

Bloque 1 · Identificación

Nombre de la herramienta y proveedor. Versión o plan contratado. Si el proveedor actúa como encargado del tratamiento, y con qué contrato. Responsable interno de la herramienta. Fechas de alta, de última revisión y de próxima revisión.

Bloque 2 · Qué lee

Fuentes de información a las que el agente accede, internas y externas. Categorías de datos personales que entran en juego, señalando si alguna es categoría especial. Permisos concedidos, en el lenguaje del propio sistema. Y los datos de terceros que no son objeto del tratamiento pero viven en los repositorios alcanzables, que la guía identifica como exposición específica [cap. VI.A].

Bloque 3 · Regla de 2

Las tres casillas de la figura 13 son si el agente trata información no controlada, si accede a información sensible y si ejecuta acciones automáticas. Se marcan las que concurren y se anota la garantía que cubre la pareja. Si concurren las tres, esa configuración no se permite. Se documenta la incidencia y se escala para corregirla [cap. V.G].

Bloque 4 · Qué recuerda

Qué persiste en memoria de trabajo y qué queda en registros. Dónde vive cada cosa, en sistemas propios o del proveedor. Plazo de conservación de cada memoria, y quién tramita las solicitudes de acceso y supresión sobre ella. Si aplica una política de no registro a nivel de componente, se anota [cap. VII.D]. Este bloque existe para que ninguna copia quede sin plazo decidido por nadie.

Bloque 5 · Qué hace

Acciones que ejecuta sin aprobación humana. Acciones irreversibles para las que se haya definido un punto de aprobación, con el rol que aprueba, atendiendo al tratamiento y al riesgo. Mecanismo de reversión, si existe. Cortacircuito que interrumpe la ejecución ante bucles o accesos masivos, y quién puede accionarlo [cap. VII.E y VII.F].

Bloque 6 · Quién responde

Supervisor designado de la herramienta, con las condiciones que la guía aconseja ponderar para que la supervisión cuente. Competencia y autoridad, preparación y formación, independencia, diligencia frente al sesgo de automatización, medios y tiempo [cap. VII.E]. Ruta de escalamiento cuando algo se desvía. Este bloque es el que impide cargar al supervisor con responsabilidades que corresponden al diseño.

Bloque 7 · Ciclo de vida

Qué ocurre con la memoria y los registros si la herramienta se retira. Control de actualizaciones, con quién decide cuándo entra una versión nueva y dónde queda el rastro del rechazo o del regreso atrás [cap. VII.F].

VI. CORRESPONDENCIA CON LAS MEDIDAS DE LA GUÍA

Cada bloque de la página se apoya en medidas ya enunciadas por la guía; el formato y sus reglas de uso son propuesta del autor. La tabla hace la correspondencia explícita, para que quede claro que la propuesta es de formato y no de doctrina.

Bloque de la página	Medida de la guía que recoge	Referencia
1 · Identificación	Gobernanza: roles asignados, relaciones con terceros formalizadas, control del despliegue y de su retirada	cap. VII.A
2 · Qué lee	Política de acceso a los datos de la organización y del usuario; minimización; exposición de datos de terceros	cap. VI.A y VII.C
3 · Regla de 2	Umbral mínimo de configuraciones admisibles del agente	cap. V.G, fig. 13
4 · Qué recuerda	Control de la memoria; no-log selectivo; plazos de retención estrictos; ejercicio de derechos sobre memorias y registros	cap. IV.C, V.E y VII.D
5 · Qué hace	Catálogos y listas blancas de servicios; puntos de control para intervención humana; reversibilidad; cortacircuitos	cap. VII.E y VII.F
6 · Quién responde	Condiciones de la supervisión humana efectiva; rutas de escalamiento; no desplazar al supervisor la responsabilidad del diseño	cap. VI.A y VII.E
7 · Ciclo de vida	Control estricto de actualizaciones con posibilidad de retorno; retirada del sistema	cap. VII.A y VII.F

VII. MODO DE EMPLEO MÍNIMO

1. Inventario. Listar las herramientas de IA con agentes que la organización usa de verdad. Sin perfeccionismo: la que se usa, entra; la que se probó, se anota como probada y retirada.
2. Relleno. Una página por herramienta, con la plantilla del anexo A. El tiempo de cumplimentación dependerá de la herramienta y del tratamiento.
3. Revisión por acontecimiento. La página se reabre cuando cambia la versión, los términos del proveedor o el alcance de permisos. La revisión con motivo no sustituye la evaluación continua ni las auditorías que correspondan [cap. VII.B].
4. Enlace con las obligaciones existentes. Lo escrito alimenta el registro de actividades y, donde proceda, la evaluación de impacto. La página no sustituye a ninguno de los dos: les sirve de borrador ordenado y de fuente de fechas.

El empleo no exige software nuevo, ni contrataciones, ni sellos. Exige honestidad sobre lo que se usa de verdad.

VIII. LÍMITES DE ESTA PROPUESTA

- La página por herramienta no certifica el cumplimiento de ninguna herramienta ni de ningún tratamiento. Es un formato de documentación, no un dictamen.
- No sustituye al registro de actividades de tratamiento, a la evaluación de impacto, a los contratos con encargados ni a ninguna obligación del RGPD. Es una pieza de trabajo interno previa a todo eso.
- No añade doctrina. Las medidas en que se apoya están en la guía; si la Agencia matiza alguna, el formato se corrige.
- Es discutible. Los nombres de los campos, su número y su granularidad son materia de propuesta. Este documento se publica para ser corregido, no para ser acatado.

Esta propuesta se publica como documento abierto en fundadorsupremo.org, junto al análisis completo de las orientaciones que le sirve de contexto. Cualquier canal oficial de aportaciones de la Agencia Española de Protección de Datos puede hacer uso de ella, total o parcialmente, sin necesidad de permiso.

Kenyi Martín Alcántara
 Editor de fundadorsupremo.org
 Madrid, 26 de septiembre de 2026

ANEXO A. PLANTILLA EN BLANCO DE LA PÁGINA POR HERRAMIENTA

Una página por herramienta de uso real. Los textos en gris pequeño son pistas de relleno, no definiciones normativas.

1 · IDENTIFICACIÓN	Herramienta y proveedor: Versión o plan: incluye fecha de la versión en uso ¿Encargado de tratamiento? Contrato: referencia y fecha Responsable interno · edición · próxima revisión:
2 · QUÉ LEE	Fuentes internas y externas: Categorías de datos personales: ¿alguna categoría especial? Permisos concedidos: en el lenguaje del propio sistema Datos de terceros alcanzables:
3 · REGLA DE 2	☐ Trata información no controlada correos entrantes, páginas web, documentos de terceros ☐ Accede a información sensible ☐ Realiza acciones automáticas Garantía que cubre la pareja: si hay tres marcas, esa configuración no se permite; se documenta y se corrige

4 · QUÉ RECUERDA	Memoria de trabajo, qué persiste: Registros, qué queda y dónde: propios o del proveedor Plazo de conservación de cada una: Quién tramita acceso y supresión: ¿existe política de no registro en algún componente?
5 · QUÉ HACE	Ejecuta sin aprobación: Acciones con punto de aprobación definido, aprueba: rol que aprueba; solo las que el tratamiento y el riesgo aconsejen marcar Reversión: Cortacircuito y quién lo acciona:
6 · QUIÉN RESPONDE	Supervisor designado: competencia y autoridad, preparación y formación, independencia, diligencia frente al sesgo de automatización, medios, tiempo Ruta de escalamiento:
7 · CICLO DE VIDA	Al retirar la herramienta, memoria y registros: ¿se recuperan, se destruyen, caducan? Control de actualizaciones: quién aprueba entrar en producción una versión nueva

Referencia de las medidas: «Inteligencia Artificial Agéntica desde la Perspectiva de Protección de Datos», V1.2, febrero de 2026, Agencia Española de Protección de Datos (www.aepd.es/guias/orientaciones-ia-agentica.pdf). Esta plantilla es una propuesta editorial independiente; no ha sido emitida ni avalada por la Agencia.