La responsabilidad proactiva diez años después: del cumplimiento documental a la protección verificable

Accountability Ten Years On: From Documentary Compliance to Verifiable Protection

Helena Duarte Avanzato
Abogada especializada en Compliance
y Protección de Datos
Busquets Law & Finance

Fecha de recepción: 20.06.2026
Fecha de aceptación: 01.08.2026
Fecha de publicación en línea: octubre 2026

Resumen:

El principio de responsabilidad proactiva (accountability) del Reglamento General de Protección de Datos exige que los responsables del tratamiento no solo cumplan con sus obligaciones, sino que puedan demostrarlo mediante controles verificables y evidencias auditables. A diez años de su aprobación, la práctica organizativa mayoritaria ha respondido a esa exigencia mediante la producción documental —registros, contratos de encargo, políticas de privacidad, evaluaciones de impacto—. La actividad sancionadora de la Agencia Española de Protección de Datos y la jurisprudencia contencioso-administrativa acreditan que la existencia de documentos no equivale a gobernanza: lo determinante es que los controles funcionen y puedan reconstruirse. Esa misma lógica alcanza a la cadena de encargo, donde la visibilidad sobre los subencargados y la continuidad de la supervisión resultan exigibles como parte del propio cumplimiento. La inteligencia artificial actúa como prueba de estrés que expone con especial nitidez las insuficiencias del modelo documental y desplaza parte de las obligaciones hacia el Reglamento de Inteligencia Artificial y la evaluación de impacto en los derechos fundamentales. El artículo defiende que la accountability efectiva requiere un auténtico sistema de gestión del riesgo, con fases definidas, comunicación y consulta, mejora continua, controles auditables y un delegado de protección de datos con acceso e independencia reales; un modelo que el ordenamiento español ya impone con carácter obligatorio en marcos como el Esquema Nacional de Seguridad.

Palabras clave:

responsabilidad proactiva; cumplimiento efectivo; gestión del riesgo; subencargados de tratamiento; inteligencia artificial.

Abstract:

The principle of accountability under the General Data Protection Regulation requires data controllers not only to comply with their obligations but to demonstrate that compliance through verifiable controls and auditable evidence. Ten years after the Regulation's adoption, most organisations have responded to this requirement through documentary production —records of processing activities, data processing agreements, privacy policies, impact assessments—. The enforcement activity of the Spanish Data Protection Agency and the administrative courts confirm that the existence of documents does not equal governance: what matters is that controls function and can be reconstructed. The same logic extends to the processing chain, where visibility over sub-processors and continuity of supervision are required as part of compliance itself. Artificial intelligence acts as a stress test that exposes the shortcomings of the documentary model with particular clarity and shifts part of the obligations towards the Artificial Intelligence Act and the fundamental rights impact assessment. This article argues that effective accountability requires a genuine risk management system, with defined phases, communication and consultation, continual improvement, auditable controls and a data protection officer with genuine access and independence; a model that Spanish law already makes mandatory in frameworks such as the National Security Framework.

Keywords:

Proactive responsibility; effective compliance; risk management; sub-processors; artificial intelligence.

Sumario:

1. Introducción. **2.** La responsabilidad proactiva como eje del modelo preventivo del RGPD. **2.1.** Origen, evolución y recepción normativa del principio. **2.2.** Contenido normativo: los artículos 5.2 y 24 RGPD y el considerando 74. **2.3.** De la obligación de cumplir a la obligación de demostrar: el cambio de paradigma. **2.4.** La responsabilidad proactiva como mandato verificable, no como principio declarativo. **3.** La brecha entre cumplimiento documental y cumplimiento efectivo. **3.1.** Las insuficiencias del modelo: cuando la documentación no equivale a control. **3.2.** La evidencia sancionadora: resoluciones de la AEPD y jurisprudencia. **3.3.** El estándar que emerge: gestión del riesgo, trazabilidad y demostrabilidad. **4.** La gobernanza de proveedores y la cadena de tratamiento: la accountability ante terceros. **4.1.** La cadena de tratamiento como vector de riesgo estructural. **4.2.** El contrato de encargo como instrumento de gobernanza, no como documento-fin. **4.3.** La imputación al encargado no exime al responsable. **4.4.** Más allá del contrato: gobernanza efectiva de proveedores. **5.** La inteligencia artificial como reveladora de las insuficiencias del modelo. **6.** Del papel a la práctica: cómo se materializa el cumplimiento efectivo en la organización. **6.1.** La accountability como sistema de gestión del riesgo: elementos y fases. **6.2.** Modelos de gestión vigentes en el ordenamiento: más allá de la voluntariedad. **6.3.** Políticas, controles, formación y reporting como instrumentos de accountability. **6.4.** El papel del Delegado de Protección de Datos (DPD). **7.** Conclusiones.

Summary:

1. *Introduction.* ***2.*** *Proactive responsibility as the cornerstone of the GDPR's preventive model.* ***2.1.*** *Origin, evolution and normative reception of the principle.* ***2.2.*** *Normative content: Articles 5(2) and 24 GDPR and Recital 74.* ***2.3.*** *From the obligation to comply to the obligation to demonstrate: the paradigm shift.* ***2.4.*** *Proactive responsibility as a verifiable mandate, not a declaratory principle.* ***3.*** *The gap between documentary compliance and effective compliance.* ***3.1.*** *The shortcomings of the model: when documentation does not equal control.* ***3.2.*** *The enforcement evidence: AEPD resolutions and case law.* ***3.3.*** *The emerging standard: risk management, traceability and demonstrability.* ***4.*** *Vendor governance and the processing chain: accountability before third parties.* ***4.1.*** *The processing chain as a structural risk vector.* ***4.2.*** *The data processing agreement as a governance instrument, not a formal end in itself.* ***4.3.*** *Attribution to the processor does not exempt the controller.* ***4.4.*** *Beyond the contract: effective vendor governance.* ***5.*** *Artificial intelligence as a revealer of the model's shortcomings.* ***6.*** *From paper to practice: how effective compliance materialises within the organisation.* ***6.1.*** *Accountability as a risk management system: elements and phases.* ***6.2.*** *Management models already binding under Spanish law: beyond voluntary adoption.* ***6.3.*** *Policies, controls, training and reporting as accountability instruments.* *6.4. The role of the Data Protection Officer (DPO).* ***7.*** *Conclusions.*

1. Introducción

El Reglamento General de Protección de Datos (RGPD), aprobado hace diez años, lleva ocho años en plena aplicación. Supuso un cambio de paradigma frente a la Directiva 95/46/CE, que hasta entonces había regido la protección de datos en la Unión Europea.

Tiempo de sobra para que las organizaciones construyeran sus registros de actividades, designaran delegados de protección de datos, formalizaran contratos de encargo y publicaran políticas de privacidad —y también para comprobar que todo ello convive con incumplimientos graves, brechas de seguridad, transferencias internacionales sin garantías y tratamientos que nadie supervisa en la práctica.

El RGPD optó por un modelo preventivo articulado en torno al principio de responsabilidad proactiva, identificado en la doctrina europea como *accountability*, que el artículo 5.2 del Reglamento concreta en una doble exigencia: cumplir y estar en condiciones de demostrarlo[1]. El propio Reglamento —considerando 74, en conexión con los artículos 5.2 y 24— desplaza hacia el responsable la carga de demostrar que ha adoptado medidas técnicas y organizativas apropiadas y que el tratamiento se ajusta a sus exigencias.

Sin embargo, entre la norma y la práctica organizativa existe una distancia que la actividad sancionadora de la Agencia Española de Protección de Datos (AEPD) ha documentado con reiteración. Registros de actividades de tratamiento desactualizados, contratos de encargo formalizados sin seguimiento real de las medidas de seguridad del encargado, evaluaciones de impacto realizadas

[1] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, DO L 119, 4.5.2016, p. 1, art. 5.2.

como trámite y no como instrumento de gestión del riesgo, ausencia de formación efectiva del personal, políticas de privacidad genéricas que no reflejan los tratamientos reales. El cumplimiento documental —tener el papel— opera, en la práctica, como un mero sustituto del cumplimiento efectivo —garantizar la protección material del derecho—: la organización cree que cumple porque conserva documentos, pero no puede demostrar que respondan a su realidad operativa.

La jurisprudencia más reciente ha empezado a corregir esa deriva. En sentencia de 26 de marzo de 2026, el Tribunal Supremo ha fijado con carácter de doctrina jurisprudencial que el responsable del tratamiento queda sujeto al cumplimiento de los principios del Reglamento desde el mismo momento en que solicita datos a una persona física, con independencia de que estos lleguen o no a ser efectivamente facilitados[2]. El cumplimiento no se activa con la recogida del dato. Se activa con la decisión de solicitarlo. El pronunciamiento consolida, en sede casacional, la lógica del principio de protección de datos desde el diseño y por defecto: la regularización documental a posteriori no subsana la ausencia de gobernanza a priori.

A esta tensión entre el cumplimiento aparente y el cumplimiento efectivo se suma un factor que la agudiza con especial claridad: la inteligencia artificial (IA). Su adopción masiva en las organizaciones —en atención al cliente, en procesos de selección de personal, en análisis crediticio y en segmentación y mercadotecnia— deja sin respuesta a la política de privacidad genérica cuando la organización no ha inventariado qué herramientas de IA utilizan sus empleados, qué datos personales se introducen en ellas, cuál es la base jurídica legitimadora de ese tratamiento, si existen encargados del tratamiento situados fuera del Espacio Económico Europeo, si se producen decisiones individuales automatizadas en el sentido del artículo 22 del Reglamento, o si el sistema genera riesgos de sesgo algorítmico, opacidad funcional o inobservancia del deber de transparencia. La inteligencia artificial no crea todos estos riesgos. Los intensifica y los vuelve difícilmente disimulables tras un repositorio documental estático.

La tesis que aquí se propone defender parte de esa constatación: el modelo documental ha llegado a un límite. No es capaz, por sí solo, de garantizar ni de demostrar que los datos personales se tratan de forma lícita, proporcional y segura en el interior de las organizaciones. Las herramientas que el propio RGPD ya contiene —enfoque basado en el riesgo, evaluaciones de impacto, medidas técnicas y organizativas, asignación de responsabilidades, documentación y revisión— necesitan algo que las traduzca en controles verificables y evidencias auditables para que la *accountability* sea real y no meramente declarativa. Ese algo lo aportan las metodologías propias del Compliance, entendido como sistema organizado de prevención, control, supervisión y mejora continua del cumplimiento normativo.

La doctrina ha estudiado el enfoque basado en el riesgo del Reglamento y, por separado, el cumplimiento normativo como sistema de gestión[3]. Este trabajo articula ambos planos: sostiene que ese sistema no es metodología importada de la práctica empresarial, sino el contenido exigible del artículo 24.1 RGPD que revela la actividad sancionadora, y un modelo que el ordenamiento español ya impone obligatoriamente fuera de la protección de datos.

2. La responsabilidad proactiva como eje del modelo preventivo del RGPD

La responsabilidad proactiva exige que las organizaciones sepan qué datos tratan, con qué finalidades y mediante qué operaciones, que determinen cómo aplicar las medidas previstas por el Reglamento y que puedan acreditar ante interesados y autoridades de supervisión que esas medidas son adecuadas.

2.1 Origen, evolución y recepción normativa del principio

El concepto de *accountability* en materia de protección de datos no nació con el RGPD. Su genealogía se remonta, al menos, a las Directrices sobre Privacidad de la OCDE de 1980, que formularon la idea de que «todo responsable de datos debería ser responsable de cumplir con las medidas

[2] Tribunal Supremo, Sala de lo Contencioso-Administrativo, Sección Tercera, sentencia núm. 390/2026, de 26 de marzo de 2026, recurso de casación núm. 6649/2024, ECLI:ES:TS:2026:1590 (CENDOJ: 28079130032026100089).

[3] Gellert, Raphaël, «The role of the risk-based approach in the General Data Protection Regulation and in the European Commission's proposed Artificial Intelligence Act: Business as usual?», *Journal of Ethics and Legal Technologies*, vol. 3, núm. 2 (2021), pp. 15-33.

que hagan efectivos los principios [materiales] expuestos»[4]. Era una formulación incipiente, sin carga sancionadora operativa, pero ya fijaba el núcleo que décadas después trasladaría el derecho positivo europeo: no basta con declarar la sujeción a unos principios; es preciso adoptar medidas concretas que los hagan efectivos.

El Grupo de Trabajo del Artículo 29 convirtió esa idea en una propuesta normativa. En su Documento de Trabajo WP168 sobre el Futuro de la Privacidad, el GT29 identificó la *accountability* como respuesta a las disfunciones de la transposición fragmentaria de la Directiva 95/46/CE —falta de efectividad de las medidas de seguridad, excesiva carga burocrática y divergencia regulatoria entre Estados miembros—[5]. Poco después, en 2010, el Dictamen 3/2010 sobre el principio de responsabilidad sistematizó sus implicaciones en una lista abierta de medidas que los responsables debían adoptar y poder acreditar. Esa lista, ejemplificativa y no exhaustiva, anticipaba la lógica del Reglamento: no un catálogo cerrado de actuaciones, sino una capacidad demostrable de cumplimiento, con los medios concretos a elección del responsable[6].

La recepción definitiva se produjo con la aprobación del Reglamento (UE) 2016/679. El texto legal no define el principio —el artículo 4 no lo incluye entre las definiciones— y la expresión «responsabilidad proactiva» solo aparece de forma expresa en el artículo 5.2 y en el considerando 85. Esa escasa presencia literal no le resta, sin embargo, papel estructural: los verbos que le dan contenido —cumplir, garantizar, demostrar, revisar— aparecen de forma recurrente a lo largo del texto y muestran que la *accountability* opera como los principios generales, ordenando la interpretación del conjunto normativo en vez de imponer una regla cerrada. No sustituye a los demás principios del tratamiento: obliga al responsable a hacerlos efectivos y a poder demostrarlo[7].

2.2 Contenido normativo: los artículos 5.2. y 24 RGPD y el considerando 74

La formulación positiva del principio se condensa en el artículo 5.2 RGPD: «el responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo ("responsabilidad proactiva")»[8]. Dos exigencias, no una. La distinción no es menor. Si el responsable no puede acreditar la conformidad del tratamiento, queda comprometido el propio deber de responsabilidad demostrable, aunque sostenga que el tratamiento era materialmente conforme.

Aunque la literalidad del artículo 5.2 pudiera sugerir que la responsabilidad proactiva se limita al cumplimiento de los principios enunciados en el apartado primero, su alcance es más amplio. La *accountability* no es una obligación sustantiva más que se suma a las demás —no impone, por sí misma, tratar los datos de forma leal o minimizarlos—, sino un principio de segundo orden que opera sobre la forma en que se cumplen los demás principios del Reglamento: no dice qué hacer materialmente, sino cómo gestionar y demostrar que se hace. Cada decisión relevante —desde la base jurídica hasta la selección de encargados, las evaluaciones de impacto o las medidas de seguridad— debe poder explicarse y acreditarse, identificando riesgos, documentando y revisando cuando cambian las circunstancias.

El artículo 24 RGPD desarrolla ese mandato en términos operativos. El responsable «aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento», y esas medidas «se revisarán y actualizarán cuando sea necesario» —artículo 24.1—. El artículo 24.2 añade las «oportunas políticas de protección de datos» como posible medida de cumplimiento; el 24.3, los mecanismos de certificación. Esa exigencia de revisión introduce una dimensión temporal decisiva: el cumplimiento no se fija en un momento inicial, sino que se mantiene mientras subsista el tratamiento.

Por su parte, el considerando 74 completa este marco y lo conecta con los elementos decisivos para el resto del análisis: riesgo, eficacia, prueba y extensión de la responsabilidad a quienes tratan datos por cuenta del responsable. Establece que el responsable «debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas», atendiendo a «la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y

[4] GT29, Dictamen 3/2010 sobre el principio de responsabilidad (WP173), adoptado el 13 de julio de 2010, p. 7. El GT29 recoge el principio formulado en las Directrices sobre Privacidad de la OCDE de 1980.

[5] GT29, Documento de Trabajo sobre el Futuro de la Privacidad (WP168), adoptado el 1 de diciembre de 2009, p. 20.

[6] GT29, WP173, op. cit., p. 12.

[7] Estepa Montero, Manuel, «El principio de responsabilidad proactiva o rendición de cuentas como informador del régimen jurídico de la protección de datos de las personas físicas», *Anuario Jurídico y Económico Escurialense* (AJEE), LV (2022), pp. 67-90.

[8] Reglamento (UE) 2016/679, op. cit., art. 5.2.

libertades de las personas físicas»[9]. Las medidas deben adecuarse al riesgo concreto, su eficacia debe acreditarse —no basta con que existan— y la responsabilidad alcanza también a los tratamientos que se ejecutan por cuenta del responsable, a través de encargados. La responsabilidad proactiva no se detiene en la organización interna: alcanza a la forma en que el responsable selecciona, instruye y supervisa a quienes tratan datos por su cuenta[10].

2.3 De la obligación de cumplir a la obligación de demostrar: el cambio de paradigma

Bajo el régimen de la Directiva 95/46/CE, el cumplimiento en materia de protección de datos descansaba en una lógica de lista: el nivel de seguridad exigido venía determinado por la categoría de datos tratados, sin que el sistema exigiera una evaluación continuada de su adecuación al riesgo real. El foco estaba en la clase de dato. La exigencia probatoria, en cambio, ocupaba un lugar secundario.

El RGPD desplaza ese enfoque: lo relevante ya no es solo la categoría del dato, sino el riesgo que el tratamiento puede generar para los derechos y libertades de las personas. El cumplimiento deja de concebirse como un estado alcanzado una vez y mantenido por inercia, y pasa a ser una práctica continuada de identificación, gestión, acreditación y revisión. Si las medidas deben ser apropiadas al riesgo, también debe poder explicarse por qué lo son: la prueba del cumplimiento deja de descansar en la mera existencia de medidas formalmente adoptadas y pasa a depender de una evaluación concreta y contextualizada. La idea puede resumirse en una fórmula que ha hecho fortuna en la doctrina española: cumplir formalmente con la norma ha dejado de ser una garantía suficiente frente al RGPD.

La jurisprudencia del Tribunal de Justicia ha precisado los efectos de esa exigencia. En la sentencia de 14 de diciembre de 2023, el TJUE declaró que la existencia de un acceso no autorizado por terceros no prueba, por sí sola, la inadecuación de las medidas técnicas y organizativas aplicadas. Esa precisión evita convertir cualquier incidente en prueba automática de incumplimiento, pero no vacía de contenido la carga de acreditación del responsable: le corresponde demostrar qué riesgos identificó, qué medidas aplicó, por qué las consideró adecuadas y cómo verificó su funcionamiento[11].

La sentencia de 25 de enero de 2024 va en la misma dirección, con un matiz: el incidente no genera una presunción automática de insuficiencia, pero obliga a examinar si las medidas adoptadas eran adecuadas en términos reales, no meramente formales. La responsabilidad proactiva se acredita con evidencias —análisis de riesgos, criterios de selección, controles de funcionamiento—, y exige, como mínimo, la adopción de medidas apropiadas al riesgo concreto y la existencia de un sistema de revisión y actualización. Ninguno de esos planos se satisface con la mera existencia de documentos[12].

La jurisprudencia nacional ha trasladado esa misma exigencia a los controles estructurales del modelo de cumplimiento. La Audiencia Nacional, en sentencia de 11 de septiembre de 2025, rechazó la regularización posterior del contrato de encargo del tratamiento y precisó que la *accountability* exige un cumplimiento efectivo y previo de los elementos básicos del sistema: la formalización escrita y tempestiva del contrato previsto en el artículo 28 RGPD no es una formalidad subsanable a posteriori, sino un control exigible desde el inicio del tratamiento[13].

2.4 La responsabilidad proactiva como mandato verificable, no como principio declarativo

La *accountability* se formuló con la apertura propia de los principios generales. Esa flexibilidad tiene un coste: facilita que se invoque como declaración de cumplimiento sin que exista detrás una realidad organizativa capaz de sostenerlo.

[9] Reglamento (UE) 2016/679, op. cit., considerando 74.

[10] Reglamento (UE) 2016/679, op. cit., arts. 28.1 y 28.4, en relación con el considerando 74.

[11] STJUE (Sala Tercera), de 14 de diciembre de 2023, asunto C-340/21, *Natsionalna agentsia za prihodite*, EU:C:2023:986, apdos. 29-32, 34, 39, 49 y ss., 57.

[12] STJUE, Sala Tercera, de 25 de enero de 2024, asunto C-687/21, *BL / MediaMarktSaturn Hagen-Iserlohn GmbH*, EU:C:2024:72, apdos. 38-45.

[13] SAN (Sala de lo Contencioso-Administrativo, Sección Primera), de 11 de septiembre de 2025, recurso núm. 16/2023, ECLI:ES:AN:2025:3842, Fundamento de Derecho Cuarto.

La respuesta del RGPD a ese riesgo no consiste en exigir más declaraciones, sino en exigir demostración. La responsabilidad proactiva no se satisface con afirmar que la organización cumple, ni con disponer de documentos que reproduzcan las obligaciones legales. Exige poder acreditar que las decisiones adoptadas responden a una evaluación real del tratamiento: qué datos se tratan, con qué finalidad, bajo qué base jurídica, con qué riesgos, mediante qué medidas y con qué controles de revisión. La diferencia no está en el volumen documental, sino en la capacidad de conectar cada documento con una decisión, cada decisión con un riesgo, y cada riesgo con una medida verificable.

Desde esa perspectiva, la distinción entre obligaciones de medios y de resultado debe manejarse con cautela. El RGPD no exige al responsable que garantice la inexistencia absoluta de incidentes o brechas de seguridad; sí le exige demostrar que adoptó medidas apropiadas al riesgo, eficaces en el contexto concreto del tratamiento, y revisadas cuando las circunstancias lo requerían. La diligencia no desaparece; queda sometida a prueba. No basta con haber actuado de forma razonable si esa razonabilidad no puede reconstruirse a partir de evidencias.

Esa exigencia probatoria no se detiene en los procesos internos de la organización. El considerando 74 alcanza también a los tratamientos realizados por cuenta del responsable: la selección, instrucción y supervisión de los encargados son parte del propio cumplimiento, como se desarrolla en el apartado cuarto. El Tribunal de Justicia ha reforzado esa extensión al vincular la responsabilidad al poder real de decisión sobre los fines y medios del tratamiento, incluso cuando quien participa en esa determinación no ejecuta materialmente las operaciones[14].

La fractura que persiste tras una década de aplicación no está en la ausencia de documentos, sino en la distancia entre los documentos que se conservan y el sistema que debería darles soporte.

3. La brecha entre cumplimiento documental y cumplimiento efectivo

Piñar Mañas advirtió que el RGPD suponía un cambio profundo en el modelo europeo de privacidad, con un desplazamiento desde la gestión de datos hacia el uso responsable de la información[15]. A diez años de su aprobación, la cuestión relevante es si esa transformación se ha incorporado realmente a la práctica organizativa. El análisis de la actividad sancionadora de la AEPD y de la jurisprudencia contencioso-administrativa más reciente muestra que esa evolución sigue siendo incompleta.

Tras su plena aplicación en mayo de 2018, muchas organizaciones respondieron al nuevo marco con producción documental. Resulta comprensible: el RGPD, diseñado con deliberada apertura en cuanto a las medidas concretas que integran la *accountability*[16], generó una incertidumbre inicial que los operadores jurídicos resolvieron apoyándose en lo que podía verificarse y exhibirse ante una inspección. La documentación ofrecía seguridad formal; los controles internos exigían una verificación más compleja.

Ahora bien, la existencia de esos instrumentos no acredita que el cumplimiento funcione en la práctica. El considerando 74 exige demostrar la eficacia de las medidas[17] y el artículo 24.1 impone revisarlas, lo que introduce una obligación de demostrabilidad continuada que la doctrina ha vinculado al ciclo de mejora continua propio de los estándares internacionales y de las metodologías de *compliance*[18]. La actividad sancionadora de la AEPD y la jurisprudencia de los últimos años reflejan esa distancia de forma sistemática, con una coherencia argumentativa suficiente para identificar un estándar emergente. Su análisis es el objeto de los subapartados que siguen.

[14] STJUE (Gran Sala), de 5 de diciembre de 2023, asunto C-683/21, *Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos*, EU:C:2023:949, párrs. 30, 36-38 y fallo, punto 1.

[15] Piñar Mañas, José Luis, «Introducción. Hacia un nuevo modelo europeo de protección de datos», en Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad, dir. José Luis Piñar Mañas, coord. María Álvarez Caro y Miguel Recio Gayo (Madrid: Reus, 2016), p. 14. Esta misma idea es recogida por Estepa Montero, op. cit.

[16] GT29, WP173, op. cit., p. 8, donde se subraya que el principio de responsabilidad no se centra tanto en la terminología utilizada como en las medidas precisas para hacerlo efectivo.

[17] Reglamento (UE) 2016/679, op. cit., considerando 74.

[18] Reglamento (UE) 2016/679, op. cit., art. 24.1. Sobre la conexión entre la revisión periódica exigida por el RGPD, los estándares ISO y las metodologías de compliance, véase García-Sotoca Barreda, Fernando-Francisco, «Derecho de protección de datos personales y análisis del riesgo: un enfoque práctico», *Revista de Derecho de la UNED (RDUNED)*, núm. 35 (2025), pp. 358-359.

3.1 Las insuficiencias del modelo: cuando la documentación no equivale a control

El artículo 30 del RGPD concibe el registro de actividades de tratamiento como instrumento de inventario y trazabilidad: cumple esa función si refleja fielmente los tratamientos de la organización y permite identificar qué datos se tratan, con qué finalidad, sobre qué base jurídica, durante cuánto tiempo, con qué destinatarios y bajo qué medidas de seguridad. Su utilidad no reside en la mera existencia del documento, sino en ordenar el conocimiento interno del responsable y servir de punto de partida para el resto de obligaciones del sistema: información a los interesados, análisis de riesgos, contratos con encargados, medidas técnicas y atención de derechos.

El propio Tribunal de Justicia de la Unión Europea ha precisado que el registro de actividades es una obligación del capítulo IV del RGPD —una medida de *accountability*—, en un plano distinto al de los principios materiales del capítulo II: su existencia no acredita por sí misma el cumplimiento de los artículos 5 y 6, ni su inexistencia basta para demostrar la vulneración del derecho fundamental. El registro es necesario para la gobernanza del tratamiento, pero no agota la demostración del cumplimiento[19].

Si el tratamiento real diverge del documentado —por ejemplo, cuando la geolocalización de trabajadores forma parte de la operativa sin que el registro recoja su alcance efectivo, o cuando los flujos de datos hacia terceros no se actualizan tras un cambio tecnológico—, el registro deja de operar como evidencia de cumplimiento: compromete la trazabilidad del tratamiento y dificulta demostrar que las decisiones del responsable responden a una evaluación real de la operativa. La AEPD ha declarado infracción en un supuesto de estas características, al constatar que el registro no describía la realidad operativa del tratamiento y que la información ofrecida a los interesados tampoco alcanzaba a reflejar su alcance real[20].

Lo mismo ocurre con las evaluaciones de impacto. El artículo 35 del RGPD configura la EIPD como mecanismo de análisis previo orientado a la decisión, y no como una pieza documental destinada a archivarse antes del inicio del tratamiento. Su función es anticipar riesgos, valorar su probabilidad e impacto, determinar medidas de mitigación y condicionar, en su caso, el diseño o incluso la viabilidad del tratamiento. Por ello, si el tratamiento evoluciona —por la incorporación de nuevas categorías de datos, nuevos encargados o nuevas funcionalidades técnicas— sin una revisión correlativa de la evaluación, la EIPD deja constancia de una realidad superada y pierde su valor como herramienta de control.

La obligación de revisión prevista en el artículo 24.1 RGPD, proyectada sobre la protección de datos desde el diseño y por defecto del artículo 25 RGPD, excluye un cumplimiento estático. Así lo evidencia la resolución PS/00410/2024, en la que la AEPD consideró insuficiente la invocación de auditorías y medidas previas cuando la brecha derivaba de una configuración por defecto de la plataforma que no fue revisada ni adaptada antes del inicio del tratamiento. En estos supuestos, la documentación de cumplimiento solo adquiere valor demostrativo si permite acreditar que las opciones de diseño, configuración y accesibilidad fueron efectivamente verificadas conforme al riesgo del tratamiento[21].

3.2 La evidencia sancionadora: resoluciones de la AEPD y jurisprudencia

El análisis anterior parte de la estructura normativa: qué exige el RGPD y por qué la documentación, por sí sola, no lo satisface. Los expedientes sancionadores de los últimos años muestran ese mismo problema desde el otro lado: qué ocurre cuando la Agencia abre un procedimiento y examina si los documentos se sostienen sobre algo real.

La resolución PS/00227/2024 lo ilustra en su dimensión contractual. La AEPD sancionó un modelo de cumplimiento aparente al constatar que el contrato de encargo no contenía el nivel de precisión exigible: faltaban la definición del tratamiento, las medidas de seguridad aplicables, los mecanismos de asistencia al responsable y el régimen de subencargo. Un contrato genérico no acreditaba, por sí solo, gobernanza efectiva ni reducción real del riesgo[22]. En términos similares, la resolución PS/00347/2023 declaró insuficiente trasladar contractualmente a un tercero la obligación de informar a los interesados, cuando no existían mecanismos internos que garantizasen que esa información se facilitaba realmente: el documento que distribuye obligaciones pierde valor probatorio

[19] STJUE (Sala Primera) de 4 de octubre de 2024, asunto C-200/23, *Agentsia po vpisvaniyata / OL*, EU:C:2024:827, apdos. 59-65.

[20] AEPD, Resolución PS/00526/2024, de 11 de marzo de 2025, Fundamentos de Derecho III y V.

[21] AEPD, Resolución PS/00410/2024, de 21 de marzo de 2026, Fundamentos de Derecho III y V.

[22] AEPD, Resolución PS/00227/2024, de 6 de febrero de 2026, Fundamento de Derecho V.

si no se acompaña de controles que aseguren su ejecución[23].

Las deficiencias de seguridad del tratamiento exponen el mismo problema con mayor nitidez. En la resolución PS/00459/2024, relativa al protocolo de verificación telefónica de identidad empleado por una comercializadora energética, la AEPD declaró la infracción del artículo 32 del RGPD e impuso una multa de un millón de euros: los datos empleados eran estáticos y fácilmente accesibles a terceros, el protocolo no fijaba criterios para determinar qué datos exigir en cada caso —la selección quedaba a discreción de cada operador— y no existía registro de las comprobaciones realizadas[24]. La AEPD fue explícita: «sin un registro adecuado, no es posible determinar si los datos proporcionados eran correctos, si la verificación fue efectiva ni si las gestiones realizadas fueron autorizadas por el titular legítimo. Esto deja al responsable sin herramientas para demostrar que se han aplicado medidas de seguridad apropiadas al nivel de riesgo en los términos exigidos por el RGPD». El artículo 32 exige medidas adecuadas al riesgo y capacidad de acreditar su aplicación, en conexión con los artículos 24 y 5.2 del RGPD. En el mismo sentido, la resolución REPOSICIÓN/PS/00136/2024 rechazó que una brecha de seguridad se atribuyera a un mero error humano cuando concurrían fallos estructurales —ausencia de cifrado, inexistencia de control de accesos, falta de trazabilidad sobre activos y usuarios— sin evidencias que sostuvieran esa explicación[25].

La jurisprudencia contencioso-administrativa ha consolidado esta exigencia con una precisión adicional: el cumplimiento documental tardío o puramente correctivo no tiene efecto retroactivo sobre una gobernanza inexistente en el momento relevante. La Audiencia Nacional declaró infracción grave la falta de contrato de encargo en tiempo y forma, aun cuando la brecha de seguridad la causara materialmente el proveedor, porque la formalización posterior no reconstruye los controles previos que el responsable debía haber implantado. La sentencia de 4 de julio de 2024 del mismo tribunal confirmó sanciones por deficiencias técnicas y organizativas en un entorno tecnológico cambiante: el cumplimiento requiere supervisión activa, no meros repositorios documentales estáticos[26]. En esa línea, el estándar que emerge no es el de una documentación formalmente completa, sino el de un cumplimiento materialmente defendible y demostrable en la práctica.

3.3 El estándar que emerge: gestión del riesgo, trazabilidad y demostrabilidad

La obligación de seguridad del artículo 32 del RGPD es una obligación de medios. El Tribunal Supremo lo precisó en sentencia de 15 de febrero de 2022: el compromiso del responsable consiste en adoptar medidas técnicas y organizativas idóneas y suficientes, y en desplegar una actividad diligente en su implantación y utilización; no se garantiza un resultado, pero tampoco basta con diseñar las medidas, pues es igualmente exigible su correcta implantación y utilización[27]. Esta delimitación, aparentemente favorable al responsable, incorpora una exigencia probatoria que con frecuencia se subestima: para acreditar la adecuación razonable de las medidas adoptadas debe poder explicarse cómo se determinaron y cómo se aplicaron. De ahí que deban identificarse e implantarse mediante un proceso de gestión del riesgo documentado y repetible, «precisamente para estar en condiciones de demostrar su eficacia e idoneidad»[28].

La *accountability* exige que los documentos respondan a una realidad operativa verificable. Esa exigencia tiene respaldo normativo expreso en el artículo 25 del RGPD, que impone integrar las medidas técnicas y organizativas adecuadas antes del tratamiento y durante su ejecución[29]. La privacidad desde el diseño opera como una decisión de arquitectura adoptada al configurar el sistema o el proceso, no como una referencia añadida ex post a la documentación contractual o interna.

Los expedientes sancionadores y la jurisprudencia examinados en el subapartado anterior muestran que el debate en sede administrativa y judicial se desplaza hacia las evidencias de funciona-

[23] AEPD, Resolución PS/00347/2023, de 3 de noviembre de 2023, Fundamento de Derecho IX.

[24] AEPD, Resolución PS/00459/2024, de 14 de enero de 2026, expediente EXP202406239, Fundamento de Derecho IV.

[25] AEPD, Resolución de recurso de reposición, expediente EXP202405365, relativo al procedimiento PS/00136/2024, de 23 de abril de 2025, Fundamento de Derecho II.

[26] SAN de 11 de septiembre de 2025, cit. en nota 13, Fundamento de Derecho Cuarto; SAN, Sala de lo Contencioso-Administrativo, Sección Primera, de 4 de julio de 2024, recurso núm. 382/2022, ECLI:ES:AN:2024:3693, Fundamentos de Derecho Segundo y Tercero.

[27] STS, Sala de lo Contencioso-Administrativo, Sección Tercera, núm. 188/2022, de 15 de febrero de 2022, ECLI:ES:TS:2022:543, Fundamento de Derecho Tercero.

[28] García-Sotoca Barreda, «Derecho de protección de datos personales y análisis del riesgo: un enfoque práctico», p. 353, con referencia a los arts. 32 y 83 y a los considerandos 74 y 83 del Reglamento (UE) 2016/679, op. cit., así como a la STJUE de 14 de diciembre de 2023, asunto C-340/21.

[29] Reglamento (UE) 2016/679, op. cit., art. 25.1.

miento: si el protocolo generaba trazabilidad, si el contrato de encargo reflejaba el tratamiento real, si la evaluación de impacto había considerado los riesgos del sistema efectivamente desplegado, si los controles implantados podían acreditarse antes del incidente y no solo después. Cuando en el expediente existe un informe de valoración de medidas técnicas y organizativas, ese documento resulta determinante para graduar la sanción, porque permite reconstruir si el responsable gestionó el riesgo o se limitó a describirlo.

4. La gobernanza de proveedores y la cadena de tratamiento: la *accountability* ante terceros

La estructura productiva contemporánea ha convertido el tratamiento de datos personales en una actividad necesariamente distribuida: las organizaciones alojan datos en plataformas en la nube, los canalizan mediante servicios de comunicación o los integran en software de terceros, y esa externalización introduce riesgos que el modelo documental no consigue neutralizar. La constancia documental no siempre permite saber cómo se ejecuta realmente el tratamiento, qué subencargados intervienen, desde qué infraestructuras se presta el servicio o qué medidas de seguridad se aplican en la práctica. La cuestión no es si el proveedor aparece documentado, sino si la organización conserva una capacidad real de dirección, verificación y reacción sobre esa parte externalizada del tratamiento. Ahí se sitúa uno de los puntos críticos de la *accountability*: convertir la relación con terceros en un ámbito gobernado, y no solo registrado.

4.1 La cadena de tratamiento como vector de riesgo estructural

El RGPD configura la relación entre responsable y encargado como uno de los núcleos de la accountability. El artículo 28.1 establece que el responsable «elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado»[30]: no es una elección libre seguida de una formalización contractual, sino una obligación de diligencia previa y verificable. El considerando 81 la concreta al referirse a encargados que acrediten «conocimientos especializados, fiabilidad y recursos» suficientes[31].

Esa diligencia sigue viva después de la selección inicial. El artículo 28.2 prohíbe al encargado recurrir a subencargados sin autorización previa por escrito del responsable, e impone informar de cualquier cambio previsto en la lista de subencargados, «dando así al responsable la oportunidad de oponerse a dichos cambios»[32]. Las Directrices 07/2020 del CEPD precisan que esa autorización general no puede limitarse a un acceso pasivo a una lista actualizable: el encargado debe comunicar cada nuevo subencargado de forma individual y con antelación suficiente para que el responsable pueda valorar y, en su caso, oponerse[33]. El artículo 28.4 cierra el diseño al exigir que el contrato entre encargado y subencargado imponga a este último «las mismas obligaciones» de protección de datos que el responsable impuso al encargado original[34]. Las Directrices del CEPD aclaran que esta equivalencia es funcional, no literal: no hace falta reproducir las mismas fórmulas, pero sí garantizar que las obligaciones sean sustancialmente idénticas en alcance y eficacia[35]. Esta arquitectura de traslación de obligaciones solo funciona si el responsable mantiene visibilidad real sobre quién trata los datos, en qué condiciones y con qué garantías.

4.2 El contrato de encargo como instrumento de gobernanza, no como documento-fin

El artículo 28.3 RGPD detalla el contenido mínimo del contrato de encargo: objeto, duración, naturaleza y finalidad del tratamiento, tipo de datos y categorías de interesados, obligaciones y derechos del responsable, instrucciones documentadas, confidencialidad, medidas de seguridad, régimen

[30] Reglamento (UE) 2016/679, op. cit., art. 28.1.

[31] Reglamento (UE) 2016/679, op. cit., considerando 81.

[32] Reglamento (UE) 2016/679, op. cit., art. 28.2.

[33] CEPD, Directrices 07/2020 sobre los conceptos de responsable del tratamiento y encargado del tratamiento en el RGPD, versión 2.0, adoptadas el 7 de julio de 2021, apdo. 152.

[34] Reglamento (UE) 2016/679, op. cit., art. 28.4.

[35] CEPD, Directrices 07/2020, op. cit., apdo. 160.

de subcontratación, asistencia al responsable en el ejercicio de derechos y en el cumplimiento de las obligaciones de los artículos 32 a 36, destino de los datos al término del servicio y colaboración en auditorías[36]. La amplitud del catálogo no responde a una lógica puramente formal: el contrato debe ordenar, con precisión suficiente, las condiciones reales en las que el encargado tratará los datos.

La práctica muestra una distancia apreciable entre esa función de gobernanza y el uso ordinario del contrato. Con frecuencia se utilizan modelos estandarizados, firmados sin evaluación específica del tratamiento y archivados sin revisión posterior, que no concretan las medidas de seguridad, no regulan el régimen de subencargo ni establecen procedimientos claros para la asistencia en incidentes, solicitudes de derechos o auditorías. Las Directrices 07/2020 del CEPD insisten en que el contrato debe especificar cómo prestará el encargado esa asistencia, no limitarse a reproducir los deberes del Reglamento.

Si el contrato se limita a replicar el artículo 28 RGPD sin conexión con el servicio contratado, difícilmente opera como evidencia de control. La gobernanza de proveedores exige que permita reconstruir el tratamiento externalizado: qué operaciones realiza el encargado, con qué medios, bajo qué instrucciones, con qué subencargados, con qué medidas de seguridad y con qué mecanismos de verificación[37].

4.3 La imputación al encargado no exime al responsable

En los procedimientos sancionadores relacionados con la cadena de encargo, el responsable intenta con frecuencia desplazar su responsabilidad hacia el encargado cuando el incidente tiene su origen inmediato en la actuación de este último. La Resolución PS/00410/2024, de 21 de marzo de 2026, lo descarta con claridad: la existencia de controles documentados o de un contrato de encargo no basta si, en la práctica, el sistema se desplegó con configuraciones inadecuadas que el responsable no verificó antes del inicio del tratamiento[38]. El argumento puede ser comprensible desde una lógica contractual, pero no resulta eficaz frente al estándar de responsabilidad proactiva del RGPD: la Agencia rechaza que la actuación del encargado neutralice, por sí sola, la responsabilidad del responsable.

Esta línea es coherente con la estructura normativa del artículo 28 RGPD. La responsabilidad del responsable puede derivarse de una selección insuficientemente diligente, de instrucciones imprecisas o de una supervisión inadecuada del encargo. La obligación de elegir únicamente encargados que ofrezcan garantías suficientes —artículo 28.1— no se cumple con la sola firma del contrato: exige evidencias de que esa evaluación se realizó antes de la contratación y de que se mantiene durante la vigencia de la relación[39].

El problema se intensifica cuando el encargado recurre a subencargados sin autorización. En la Resolución PS/00080/2024, una cadena de subcontrataciones sucesivas realizadas sin autorización previa y por escrito, y sin contratos de subencargo que trasladaran las obligaciones del artículo 28.4, llevó a la AEPD a apreciar tres infracciones autónomas del artículo 28 y a rechazar la alegación de doble sanción por tratarse de hechos distintos[40]. En expediente separado sancionó al primer subencargado por dos infracciones más[41], y la Resolución PS/00251/2025 alcanza idéntica conclusión respecto de servicios de alojamiento en la nube contratados sin autorización previa[42]. La cadena, así, no diluye la responsabilidad: la multiplica en cada eslabón.

Estas resoluciones muestran que las obligaciones del artículo 28 RGPD no operan como exigencias meramente formales ni se agotan en el primer contrato de encargo: alcanzan a cada relación sucesiva de la cadena y exigen que cada intervención de terceros conserve una base jurídica, contractual y operativa verificable. El responsable que acredita sus controles internos pero no la forma en que gobierna a quienes tratan datos por su cuenta deja sin cubrir una zona esencial del riesgo.

[36] Reglamento (UE) 2016/679, op. cit., art. 28.3, letras a)-h.

[37] Reglamento (UE) 2016/679, op. cit., art. 5.2.

[38] AEPD, Resolución PS/00410/2024, **cit. en nota 21**, Fundamentos de Derecho III y V.

[39] Reglamento (UE) 2016/679, op. cit., art. 28.1, en relación con el considerando 81.

[40] AEPD, Resolución PS/00080/2024, expediente EXP202311075, Fundamentos de Derecho V, VII y IX, y parte dispositiva primera.

[41] AEPD, Resolución PS/00058/2025, expediente EXP202501866, Fundamentos de Derecho V, VII y IX, y parte dispositiva primera.

[42] AEPD, Resolución PS/00251/2025, expediente EXP202402268, Fundamentos de Derecho V y VIII, y parte dispositiva primera.

4.4 Más allá del contrato: gobernanza efectiva de proveedores

Firmar el contrato de encargo y comprobar que contiene las menciones exigidas por el artículo 28.3 RGPD no cierra la gobernanza de la cadena de tratamiento. El responsable debe conservar, durante toda la vigencia de la relación, una capacidad real de dirección, verificación y reacción sobre el tratamiento que el encargado ejecuta por su cuenta.

Antes de contratar, esa capacidad se traduce en la evaluación de las garantías del proveedor. Al contratar, exige definir operativamente las medidas y los mecanismos de control. Y mientras dura el servicio, exige una supervisión capaz de detectar cambios, incumplimientos o desviaciones relevantes.

En la fase previa, la revisión suele centrarse en comprobar que el proveedor dispone de documentación de cumplimiento —política de privacidad, registro de actividades o certificaciones de seguridad—. Esa comprobación puede ser útil, pero no sustituye la evaluación exigida por el artículo 28.1 RGPD. Lo relevante es determinar si el encargado ofrece garantías suficientes para aplicar medidas técnicas y organizativas apropiadas al tratamiento concreto que se va a externalizar, atendiendo a la capacidad técnica del proveedor, al régimen de subcontrataciones, a la ubicación geográfica del tratamiento y sus eventuales implicaciones en materia de transferencias internacionales, y a la adecuación de las medidas de seguridad frente a los riesgos específicos del encargo[43].

La fase contractual requiere que el acuerdo incorpore mecanismos que permitan verificar el cumplimiento durante la ejecución del servicio. El contrato debe prever, cuando el tratamiento lo justifique, procedimientos de auditoría definidos, obligaciones de reporte periódico, protocolos de notificación de brechas con plazos y canales concretos, reglas sobre subencargados y criterios para revisar o resolver la relación si el encargado incumple sus obligaciones. La Resolución PS/00001/2025, de 23 de noviembre de 2025, ilustra esta exigencia: la AEPD constató que el contrato entre la entidad bancaria responsable y su encargado no incluía medidas relativas a la trazabilidad de los envíos de documentación, y que el responsable desconocía incluso la identidad de los encargados que intervenían en el momento en que se produjo el extravío de la documentación personal del reclamante. La Agencia rechazó que el estándar habitual del sector justificara esa ausencia y recordó que las medidas deben adecuarse al riesgo concreto del tratamiento, apreciando infracción del artículo 32 RGPD en conexión con los artículos 5.2 y 24 RGPD[44].

La supervisión posterior es el punto en el que con mayor facilidad se debilita la gobernanza. Una vez firmado el contrato y completada la evaluación inicial, el responsable puede considerar cerrado el control del proveedor aunque el tratamiento siga desplegándose fuera de su perímetro. La obligación de revisión y actualización del artículo 24.1 RGPD alcanza también a la cadena de encargo: las garantías iniciales pueden deteriorarse, los subencargados variar, las condiciones técnicas modificarse y el tratamiento evolucionar más allá de lo previsto en el contrato original. La diligencia debida sobre proveedores directos e indirectos constituye, también en el ámbito del cumplimiento normativo, un elemento estructural del sistema y no un añadido contractual[45].

5. La inteligencia artificial como reveladora de las insuficiencias del modelo

La inteligencia artificial no ha creado las insuficiencias del modelo documental; ya existían. Simplemente ha hecho más difícil ignorarlas. Al incorporar sistemas capaces de seleccionar candidatos, gestionar reclamaciones, perfilar clientes o automatizar decisiones de negocio, la organización deja de poder sostener, sin más, que una cláusula informativa y un contrato de encargo bastan para demostrar control.

El punto de fricción aparece con especial nitidez en el artículo 22 del RGPD, que reconoce al interesado el derecho a no quedar sometido a una decisión basada únicamente en tratamientos automatizados, incluida la elaboración de perfiles, cuando produzca efectos jurídicos o le afecte de modo significativamente similar. El Grupo de Trabajo del Artículo 29 ya advirtió en sus Directrices

[43] Reglamento (UE) 2016/679, op. cit., art. 28.1, en relación con el considerando 81; CEPD, Directrices 07/2020, op. cit., apdo. 129.

[44] AEPD, Resolución PS/00001/2025, expediente EXP202500113, Fundamentos de Derecho V y VII, y parte dispositiva primera.

[45] Nieto Martín, Adán, «Cumplimiento normativo», en De la Mata Barranco, Norberto J., Dopico Gómez-Aller, Jacobo, Lascuraín Sánchez, Juan Antonio y Nieto Martín, Adán, Derecho penal económico y de la empresa, Madrid, Dykinson, 2024, pp. 221-243, esp. p. 243.

sobre decisiones individuales automatizadas y elaboración de perfiles que estos procesos «pueden ser opacos» y que «las personas no sean conscientes de que se está creando un perfil sobre ellas o que no entiendan lo que implica»; también alertó de que la elaboración de perfiles puede «llevar a predicciones inexactas» y a «la denegación de servicios y bienes, y a una discriminación injustificada»[46]. De ahí que el RGPD no se conforme con una declaración formal de transparencia: exige garantías específicas y, cuando concurren las condiciones del artículo 35.3.a), una evaluación de impacto previa[47]. Un responsable con una política informativa estándar, un encargo sin previsiones técnicas y un registro de actividades desactualizado no acredita que sabe qué hace el sistema, qué datos intervienen en cada inferencia, qué lógica condiciona el resultado ni qué efectos recaen sobre personas concretas. Hay expediente; no necesariamente cumplimiento.

Conviene precisar, sin embargo, qué obligaciones derivan del Reglamento y cuáles encuentran hoy fundamento autónomo en el Reglamento (UE) 2024/1689. El RGPD opera sobre el tratamiento de datos personales y su enfoque de riesgo se orienta a un cumplimiento demostrable; el Reglamento de Inteligencia Artificial parte de un enfoque distinto, dirigido a determinar qué sistemas quedan sujetos a regulación y con qué intensidad, y sus obligaciones recaen sobre proveedores y responsables del despliegue con independencia de que traten datos personales. La doctrina ha subrayado que se trata de dos iteraciones de un mismo modelo regulatorio basado en el riesgo: una orientada al mejor cumplimiento, otra a la delimitación del ámbito regulado[48]. La consecuencia práctica es que un mismo sistema puede exigir simultáneamente una evaluación de impacto relativa a la protección de datos, conforme al artículo 35 RGPD, y las obligaciones de gestión del riesgo que el Reglamento de Inteligencia Artificial impone a los sistemas de alto riesgo.

A esa duplicidad se añade una figura que el modelo documental no contempla: la evaluación de impacto sobre los derechos fundamentales. Su fundamento no está en el RGPD, sino en el Reglamento de Inteligencia Artificial, y su objeto es más amplio que el de la evaluación de impacto relativa a la protección de datos, pues no se limita a los riesgos para la protección de datos sino que alcanza al conjunto de derechos que el sistema puede comprometer. La distinción importa porque una evaluación correctamente realizada conforme al artículo 35 RGPD no satisface por sí sola esa exigencia. Las autoridades de control han empezado a suplir esa indeterminación por su cuenta: la Autoridad Catalana de Protección de Datos ha publicado un modelo estructurado en tres fases —planificación y determinación del alcance, recopilación de datos y análisis de riesgos, y gestión de riesgos—[49], y el Consejo de Transparencia y Protección de Datos de Andalucía ha desarrollado una herramienta metodológica propia, con niveles de exigencia graduados según el impacto del sistema. Que dos autoridades españolas construyan en paralelo metodologías distintas para una misma obligación anticipa el problema que se agrava un escalón más arriba.[50] A ello se suma un panorama de estándares todavía fragmentado —ISO/IEC 42001:2023 sobre sistemas de gestión de la inteligencia artificial, ISO/IEC 23894:2023 sobre gestión del riesgo en inteligencia artificial e ISO/IEC 42005:2025 sobre evaluación de impacto de los sistemas de IA—, cuya proliferación confirma que la respuesta regulatoria se articula sobre sistemas de gestión y no sobre documentos aislados.

La IA agéntica tensiona aún más esa insuficiencia. La Agencia Española de Protección de Datos ha advertido en sus Orientaciones sobre inteligencia artificial agéntica de 2026 que estos agentes actúan con autonomía, sin instrucciones explícitas de un operador humano, y pueden decidir cómo ejecutar tareas, qué fuentes consultar, qué información incorporar y qué acciones emprender. Esa autonomía puede desembocar en decisiones automatizadas en el sentido del artículo 22 del RGPD, incluso cuando el responsable no lo había previsto al diseñar el tratamiento. El mismo documento subraya otro riesgo: cuando un sistema agéntico sirve para implementar distintos tratamientos, sus componentes —en particular los modelos de lenguaje— pueden convertirse en puntos de recopilación de información personal procedente de varios flujos, con mayor exposición a perfilados no previstos y a daños relevantes en caso de brecha, sobre todo si intervienen servicios externos

[46] GT29, Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679 (WP251rev.01), revisadas y adoptadas el 6 de febrero de 2018, p. 6.

[47] Reglamento (UE) 2016/679, op. cit., art. 35.3.a); García-Sotoca Barreda, cit. en nota 28, pp. 358-359.

[48] Gellert, op. cit., pp. 17-31.

[49] Mantelero, Alessandro, y Joana Marí (coords.), *Modelo para la EIDF: guía y casos de uso. Metodología aplicada de la evaluación de impacto sobre los derechos fundamentales en el diseño y desarrollo de la IA*, Barcelona, Autoritat Catalana de Protecció de Dades, 2025. Sobre los modelos comparados de evaluación de impacto en derechos fundamentales, Simón Castellano, Pere, «L'avaluació d'impacte en els drets fonamentals de l'ús d'intel·ligència artificial en el sector públic: models i metodologies en perspectiva comparada», Revista Catalana de Dret Públic, núm. 71 (2025), pp. 4-24..

[50] Consejo de Transparencia y Protección de Datos de Andalucía, metodología y herramienta para el uso responsable de la inteligencia artificial en las administraciones públicas, 2026, disponible en https://www.ctpdandalucia.es/area-de-proteccion-de-datos/proteccion-datos-en-ia [consulta: 25 de julio de 2026].

gestionados por terceros[51]. La cadena deja entonces de ser lineal. Aparecen capas técnicas, registros de actividad, reutilizaciones posibles, transferencias internacionales no siempre evidentes e inferencias sobre datos especialmente sensibles. Frente a ese escenario, un contrato de encargo estándar describe una relación jurídica; no demuestra por sí solo que el tratamiento esté dominado.

Tampoco basta con una EIPD realizada una vez y archivada antes del despliegue. Las Orientaciones de la AEPD vinculan la incorporación de IA agéntica a un tratamiento preexistente con una revisión íntegra de cumplimiento, y exigen que la supervisión de los procesos automatizados sea tan continua como la automatización que se pretende controlar, apoyada en evidencias y en criterios objetivos de transparencia, reproducibilidad, control y trazabilidad[52]. Si el razonamiento interno del sistema no es directamente observable, la protección solo puede verificarse mediante capacidades efectivas de supervisión, auditoría y corrección. Sin esas capacidades, el documento que las proclama pierde valor probatorio.

La IA, por tanto, no es la causa de la crisis del modelo documental. Es el instrumento que la deja al descubierto: allí donde el responsable solo puede enseñar papeles, pero no evidencias de control, la *accountability* queda reducida a una apariencia.

6. Del papel a la práctica: cómo se materializa el cumplimiento efectivo en la organización

La brecha ya no se sitúa solo entre documentación y realidad, sino entre un cumplimiento que puede exhibirse y un cumplimiento que puede comprobarse. El artículo 24.1 RGPD identifica los instrumentos —medidas técnicas y organizativas, revisión y actualización— y el artículo 24.2 contempla las políticas de protección de datos como posible expresión de esas medidas.

6.1 La accountability como sistema de gestión del riesgo: elementos y fases

La responsabilidad proactiva no es el nombre de una política de privacidad. Describe un sistema de gestión del riesgo basado en decisiones justificadas, controles efectivos y evidencias auditables. El Reglamento no impone un modelo único para construirlo, pero sí exige que exista y que pueda ser demostrado.

Ese sistema exige, cuando menos, cuatro cosas: conocimiento actualizado de los tratamientos y de sus riesgos, determinación explícita de las medidas técnicas y organizativas adecuadas, conservación de evidencias que permitan acreditar su implantación y funcionamiento, y un sistema de revisión que evite que el cumplimiento quede congelado en el momento inicial. El artículo 24.1 articula, en rigor, cuatro verbos acumulados —cumplir, demostrar, revisar y actualizar—, y el modelo documental responde solo a los dos primeros.

Llevado al proceso, supone identificar tratamientos y activos, evaluar amenazas y su probabilidad e impacto, determinar controles proporcionales, implantarlos, verificar su funcionamiento y revisarlos cuando el tratamiento o el entorno cambian. Los estándares de gestión del riesgo añaden a esa secuencia dos elementos que el modelo documental rara vez incorpora. El primero es la comunicación y consulta con las partes interesadas, que el Reglamento traduce en la consulta previa a la autoridad de control cuando el riesgo alto no puede mitigarse —artículo 36—, en la obligación de recabar la opinión de los interesados cuando proceda —artículo 35.9— y en la posición del delegado de protección de datos como interlocutor del sistema. El segundo es la mejora continua: el resultado de la verificación debe realimentar la planificación siguiente, que es precisamente lo que impone el artículo 24.1 al ordenar que las medidas se revisen y actualicen[53]. Sin esos dos elementos hay documentación; no hay sistema.

[51] AEPD, *Orientaciones sobre inteligencia artificial agéntica desde la perspectiva de protección de datos*, versión 1.2, febrero de 2026, pp. 27-28.

[52] AEPD, *Orientaciones sobre inteligencia artificial agéntica*, op. cit., pp. 44 y 57.

[53] Asociación Española de Normalización, *UNE-ISO 31000 Gestión del riesgo. Directrices*, Madrid, AENOR, 2018, pp. 14-16. Sobre su proyección en el ámbito de la protección de datos, García-Sotoca Barreda, Fernando-Francisco, *Derecho de protección de datos personales y análisis del riesgo: un enfoque práctico*, tesis doctoral, Universidad Nacional de Educación a Distancia, 2025, cap. IV.

6.2 Modelos de gestión vigentes en el ordenamiento: más allá de la voluntariedad

Podría objetarse que este modelo describe una buena práctica organizativa sin anclaje normativo. La objeción no se sostiene: el ordenamiento español ya impone sistemas de gestión del riesgo con carácter obligatorio en ámbitos materialmente próximos. El Esquema Nacional de Seguridad, previsto en el artículo 156 de la Ley 40/2015 y regulado por el Real Decreto 311/2022, articula un sistema de obligado cumplimiento construido sobre el análisis de riesgos, la categorización de los sistemas, la implantación de medidas proporcionadas a esa categorización, la auditoría periódica y la revisión continuada; y la información que protege comprende los datos personales tratados por medios electrónicos[54]. A ese marco se asocia MAGERIT, metodología que desarrolla el análisis y la gestión de riesgos en fases definidas[55].

La misma lógica opera en el régimen de responsabilidad penal de las personas jurídicas: el artículo 31 bis del Código Penal condiciona la exención a que el modelo de organización haya sido adoptado y ejecutado con eficacia, y exige que identifique las actividades de riesgo, establezca canales de información sobre incumplimientos y se someta a verificación periódica y a modificación cuando se pongan de manifiesto infracciones relevantes o cambios en la organización[56]. A la luz de lo anterior, los estándares voluntarios adquieren su verdadera función: normas como la ISO 27001, la ISO 27701 o la ISO 31000 no son exigibles por el RGPD, pero ofrecen estructuras contrastadas para materializar lo que el Reglamento requiere sin prescribir. Su valor no reside en el certificado, que por sí solo nada demuestra, sino en la disciplina metodológica que su implantación efectiva impone.

6.3 Políticas, controles, formación y *reporting* como instrumentos de *accountability*

Las políticas internas de protección de datos cumplen su función cuando definen, con suficiente concreción, qué tratamientos se realizan, bajo qué condiciones, con qué límites y mediante qué procedimientos de revisión. Su utilidad no reside en reproducir el articulado del Reglamento en formato corporativo, sino en permitir reconstruir las decisiones de cumplimiento adoptadas por la organización. Una política que no permite esa reconstrucción difícilmente acredita gobernanza: enuncia intenciones.

Los controles técnicos y organizativos deben permitir comprobar que las medidas no solo existen, sino que funcionan: cifrado aplicado, gestión de accesos con registros auditables, procedimientos de notificación de brechas con plazos y responsables definidos, revisiones documentadas[57].

La formación del personal reduce el riesgo humano cuando alcanza a quienes intervienen realmente en las operaciones de tratamiento. El artículo 39.1.b) RGPD encomienda al DPD supervisar, entre otros elementos, la concienciación y formación del personal que participa en dichas operaciones. Si la formación no llega a quienes deciden sobre datos, deja sin cubrir una de las zonas en las que con mayor frecuencia se originan los incumplimientos. Una formación acreditable —con registros de asistencia, verificación de comprensión y periodicidad adecuada al riesgo del puesto— constituye evidencia de cumplimiento. Un correo de difusión masiva, por sí solo, no.

El reporting interno permite que el sistema no opere a ciegas. Incidentes, cambios tecnológicos no evaluados o modificaciones en los tratamientos deben llegar a quien tiene capacidad de decisión. Sin ese flujo de información, la revisión y actualización que exige el artículo 24.1 RGPD queda debilitada. El reporte no debe concebirse como un informe anual, sino como la condición para que el modelo no quede congelado.

6.4 El papel del Delegado de Protección de Datos (DPD)

El Delegado de Protección de Datos (DPD) es la figura mediante la cual el RGPD articula, desde el interior de la organización, la supervisión del sistema de cumplimiento. El Grupo de Trabajo del Artículo 29 lo describió como «la piedra angular de la rendición de cuentas» y precisó que su nombramiento puede facilitar el cumplimiento y convertirse en una ventaja competitiva para las organizaciones[58].

[54] Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, BOE núm. 106, de 4 de mayo de 2022, dictado en desarrollo del art. 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

[55] Ministerio de Hacienda y Administraciones Públicas, *MAGERIT versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método*, Madrid, 2012.

[56] Nieto Martín, op. cit., pp. 232-233.

[57] García-Sotoca Barreda, cit. en nota 28, pp. 358-359.

[58] GT29, Directrices sobre los delegados de protección de datos (DPD) (WP243rev.01), revisadas y adoptadas el 5 de abril de 2017, p. 4.

El artículo 39 RGPD le asigna funciones concretas: informar y asesorar al responsable y a los empleados (art. 39.1.a); supervisar el cumplimiento del Reglamento y de las políticas internas, incluidas la asignación de responsabilidades, la formación y las auditorías (art. 39.1.b); asesorar sobre evaluaciones de impacto (art. 39.1.c); y cooperar con la autoridad de control (arts. 39.1.d y e). Para que esa función sea real, el Reglamento exige participación adecuada y oportuna en todas las cuestiones relativas a protección de datos, recursos necesarios, acceso a los datos y operaciones de tratamiento, y ausencia de instrucciones en el desempeño de sus funciones (art. 38.1, 2 y 3).

La independencia funcional es la condición que hace posible la supervisión. El GT29 subrayó que «el nombramiento de un DPD es un primer paso, pero el DPD debe contar además con la autonomía y los recursos suficientes para desarrollar su labor de forma efectiva»[59]. Un DPD sin acceso real a la operativa, sin participación en el diseño de nuevos tratamientos y sin recursos suficientes para auditar el sistema puede firmar documentos, pero no supervisar el cumplimiento.

Supervisar la observancia del Reglamento no convierte al DPD en responsable personal de los incumplimientos: corresponde al responsable del tratamiento garantizar y demostrar la conformidad del tratamiento con el Reglamento. El DPD no sustituye esa responsabilidad; la somete a control interno. Su posición es un indicador institucional del modelo de cumplimiento: con acceso real, independencia garantizada y recursos adecuados, su existencia acredita que la organización ha construido algo más que un repositorio documental; sin esas condiciones, la designación apenas altera la realidad del cumplimiento. La diferencia no está en el certificado de nombramiento, sino en la capacidad efectiva de detectar, informar y corregir[60].

7. Conclusiones

Diez años después de su aprobación, el RGPD ha producido organizaciones ampliamente documentadas, aunque no siempre capaces de trasladar esa documentación a un cumplimiento efectivo. La brecha no responde solo a defectos puntuales de implantación; presenta una dimensión estructural. El modelo documental que se consolidó tras mayo de 2018 respondió a la incertidumbre inicial con aquello que podía conservarse y exhibirse —registros, contratos, políticas, evaluaciones de impacto archivadas—, pero ese enfoque descansaba en una lógica de cobertura formal que el propio Reglamento rechaza desde su diseño.

Lo que el artículo 5.2 del RGPD exige —cumplir y poder demostrarlo— articula una doble obligación que va más allá de la producción documental. El considerando 74 precisa que debe acreditarse la eficacia de las medidas, no su mera existencia; y el artículo 24.1 incorpora la revisión y actualización como componente permanente del sistema. Cumplimiento, demostrabilidad y revisión no remiten a un archivo estático, sino a una forma de gestión.

La actividad sancionadora de la AEPD y la jurisprudencia contencioso-administrativa han concretado ese estándar con una coherencia creciente. Un contrato de encargo que no refleja el tratamiento real, una evaluación de impacto que no se revisa tras un cambio tecnológico o un protocolo de verificación sin trazabilidad dejan al responsable sin herramientas para demostrar que las medidas aplicadas eran apropiadas al riesgo. Tampoco el cumplimiento posterior a un incidente reconstruye la gobernanza que debía existir antes.

La misma insuficiencia aparece fuera del perímetro interno de la organización. Un responsable que no puede reconstruir quién trata sus datos, bajo qué condiciones y con qué subencargados no está en condiciones de demostrar la conformidad que el artículo 5.2 le exige. La cadena de encargo forma parte del propio sistema de cumplimiento del responsable, aunque su ejecución material se desplace a terceros.

A esa tensión entre documentación y control efectivo, la inteligencia artificial añade una dimensión de escrutinio que el modelo documental no puede absorber por sí solo. Cuando el responsable solo puede aportar documentación formal, pero no evidencias de control sobre lo que el sistema decide, infiere o transfiere, las insuficiencias dejan de ser una objeción teórica y se convierten en un riesgo real y verificable.

El modelo de cumplimiento efectivo que el apartado sexto desarrolla no añade nada externo al Reglamento: operativiza lo que el artículo 24.1 ya exige. Políticas capaces de reconstruir decisiones, controles técnicos auditables, formación acreditable, flujos de información que lleguen a quien

[59] GT29, Directrices sobre los delegados de protección de datos (DPD), op. cit., pp. 4-5.

[60] GT29, Directrices sobre los delegados de protección de datos (DPD), op. cit., p. 4; Reglamento (UE) 2016/679, op. cit., art. 24.1.

decide y un DPD con acceso e independencia reales. La metodología del *compliance* no se importa desde fuera del sistema: está implícita en la propia lógica del Reglamento desde su considerando 74.

Hasta aquí, los resultados que el análisis normativo, jurisprudencial y sancionador permite acreditar. En el plano de las propuestas, la principal es organizativa antes que normativa: el Reglamento no necesita reforma para exigir un sistema de gestión, sino una práctica que lo construya y una supervisión que lo verifique.

Tratada como sistema de gestión del riesgo, y no como repositorio documental, la *accountability* transforma también la función de la supervisión regulatoria. Una autoridad de control que examina evidencias de funcionamiento —trazabilidad, revisiones, criterios documentados de decisión— no constata solo incumplimientos formales: valora si el cumplimiento opera en la práctica. Ese desplazamiento del foco regulatorio, ya visible en la jurisprudencia más reciente, exige que las organizaciones respondan con estructuras capaces de ser auditadas. La protección de los derechos de las personas físicas no se garantiza mediante un archivo ordenado; se acredita mediante un sistema capaz de funcionar y de demostrar que funciona.

Bibliografía

Estepa Montero, Manuel. "El principio de responsabilidad proactiva o rendición de cuentas como informador del régimen jurídico de la protección de datos de las personas físicas." *Anuario Jurídico y Económico Escurialense LV* (2022): 67–90.

García-Sotoca Barreda, Fernando-Francisco. "Derecho de protección de datos personales y análisis del riesgo: un enfoque práctico." *Revista de Derecho de la UNED (RDUNED)*, núm. 35 (2025): 337–371.

García-Sotoca Barreda, Fernando-Francisco. *Derecho de protección de datos personales y análisis del riesgo: un enfoque práctico*. Tesis doctoral, Universidad Nacional de Educación a Distancia, 2025.

Gellert, Raphaël. "The role of the risk-based approach in the General Data Protection Regulation and in the European Commission's proposed Artificial Intelligence Act: Business as usual?" *Journal of Ethics and Legal Technologies* 3, n.º 2 (2021): 15–33.

Grupo de Trabajo del Artículo 29. Dictamen 3/2010 sobre el principio de responsabilidad (WP173). Adoptado el 13 de julio de 2010.

Grupo de Trabajo del Artículo 29. Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679 (WP251rev.01). Revisadas y adoptadas el 6 de febrero de 2018.

Grupo de Trabajo del Artículo 29. Directrices sobre los delegados de protección de datos (DPD) (WP243rev.01). Revisadas y adoptadas el 5 de abril de 2017.

Grupo de Trabajo del Artículo 29. The Future of Privacy: Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data (WP168). Adoptado el 1 de diciembre de 2009.

Mantelero, Alessandro, y Joana Marí, coords. Modelo para la EIDF: guía y casos de uso. *Metodología aplicada de la evaluación de impacto sobre los derechos fundamentales en el diseño y desarrollo de la IA*. Barcelona: Autoritat Catalana de Protecció de Dades, 2025.

Nieto Martín, Adán. "Cumplimiento normativo." En De la Mata Barranco, Norberto J., Jacobo Dopico Gómez-Aller, Juan Antonio Lascuraín Sánchez y Adán Nieto Martín, Derecho penal económico y de la empresa, 221–243. Madrid: Dykinson, 2024.

Piñar Mañas, José Luis. "Introducción. Hacia un nuevo modelo europeo de protección de datos." En *Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad*, dirigido por José Luis Piñar Mañas y coordinado por María Álvarez Caro y Miguel Recio Gayo, 11–18. Madrid: Reus, 2016.

Simón Castellano, Pere. "L'avaluació d'impacte en els drets fonamentals de l'ús d'intel·ligència artificial en el sector públic: models i metodologies en perspectiva comparada." *Revista Catalana de Dret Públic*, núm. 71 (2025): 4–24.