



CONSEJO ASESOR
DE TRANSFORMACIÓN DIGITAL

Resumen consolidado de la revisión de las empresas del Consejo

**“ANTEPROYECTO DE LEY DE LA ADMINISTRACIÓN DIGITAL
E INTELIGENCIA ARTIFICIAL DE LA COMUNIDAD DE
MADRID”**



El conjunto de aportaciones de las 16 empresas participantes presenta un alto nivel técnico, constructivo y alineado con la estrategia europea. Existe un respaldo general al Anteproyecto, acompañado de advertencias claras sobre riesgos regulatorios, operativos y de coherencia normativa.

Asimismo, se constató el reconocimiento al hecho de que la Administración haya promovido un proceso de contraste con empresas y agentes del sector durante la fase de elaboración del anteproyecto, tanto mediante aportaciones por escrito como a través de reuniones específicas. Este enfoque fue considerado positivamente, al permitir recoger observaciones técnicas y operativas en una fase temprana del proceso normativo.

1. VALORACIÓN GENERAL DEL ANTEPROYECTO

Las empresas coinciden en que:

- Supone un avance estratégico relevante.
- Refuerza el liderazgo digital de la Comunidad de Madrid.
- Está conceptualmente alineado con el AI Act.
- Integra una arquitectura institucional ambiciosa (Oficina Técnica, Consejo, Comité Ético, Registro IA).
- Equilibra impulso transformador y garantías jurídicas.

De manera ampliamente coincidente, las empresas participantes realizan una valoración positiva tanto de la iniciativa de impulsar una Ley específica en materia de administración digital e inteligencia artificial como del carácter ambicioso y amplio del texto presentado. Se destaca que la norma aborda de forma integral los principales retos de la transformación digital del sector público y que constituye una oportunidad para dotar de coherencia y marco estratégico a las actuaciones en este ámbito.

No obstante, se advierte que requiere ajustes para convertirse en un régimen plenamente operable y jurídicamente robusto y se hacen numerosas recomendaciones y sugerencias.



2. PRINCIPAL PREOCUPACIÓN TRANSVERSAL: ARMONIZACIÓN CON EL AI ACT Y MARCO EUROPEO

Este es el eje más repetido en todas las aportaciones.

Se subraya que:

- El AI Act es de aplicación directa y armonización plena.
- La norma autonómica no debe reproducir obligaciones ya establecidas en el reglamento europeo.
- Existe riesgo de:
 - Fragmentación regulatoria.
 - Duplicidades de registros.
 - Capas adicionales de evaluación.
 - Incremento de costes de cumplimiento.

Se solicita:

- Remisión expresa al AI Act en materias sustantivas.
- Limitar la ley autonómica a aspectos organizativos y procedimentales.
- Evitar divergencias terminológicas o conceptuales. En especial las relacionadas con la terminología de RIESGO – alto/Medio/Bajo- del AI Act y nuestra terminología de IMPACTO -alto/medio/bajo- no definido ni detallado en la ley

También se recomienda revisar menciones normativas por la iniciativa europea de simplificación (“Digital Omnibus”).

3. GOBERNANZA DE LA IA Y MODELO ORGANIZATIVO

Valoración positiva del modelo institucional (Oficina Técnica, Consejo, Comité Ético).

Pero se advierte la necesidad de:

- Evitar solapamientos competenciales.
- Definir un RACI claro entre órganos.
- Establecer un “circuito único” de aprobación de sistemas IA.
- Implantar gestión formal de incidencias IA (parada/rollback).



- Gobernanza del portafolio de proyectos IA.
- Informe periódico de madurez digital.
- Asegurar por ley la independencia del Comité de Ética

Se propone alineación con estándares internacionales (ISO/IEC 42001, NIST AI RMF).

4. GOBIERNO DEL DATO Y COMPARTICIÓN DE INFORMACIÓN

Se reconoce positivamente el enfoque transversal del gobierno del dato.

No obstante, se identifican riesgos:

- Falta de distinción clara entre datos públicos institucionales y datos privados aportados por empresas. En especial a lo tocante en la necesidad de transparencia y publicidad para el ciudadano de los algoritmos y modelos.
- Riesgo de afectar secreto empresarial, propiedad intelectual y confidencialidad e inhibir a las empresas de integrar sus soluciones, algoritmos y modelos en la administración pública.
- Se reconoce la oportunidad de implantar el criterio “solo una vez” de manera efectiva

Se propone:

- Limitar la compartición y publicidad obligatoria en aquellos modelos no desarrollados o propiedad exclusiva de la Administración.
 - Excluir datos protegidos por secreto empresarial.
 - Garantizar base jurídica suficiente para reutilización.
 - Garantizar la trazabilidad en la aplicación del criterio “solo una vez” y en la compartición de datos entre áreas.
-

5. INTEROPERABILIDAD Y RELACIÓN CON EL ECOSISTEMA EMPRESARIAL

Se solicita:

- Estándares técnicos abiertos.
- APIs públicas.
- Integración bidireccional con software empresarial.
- Evitar duplicidades funcionales.



También se insiste en gobernanza API, catálogo, versionado y SLAs.

La preocupación central: que la Administración no cree soluciones paralelas desconectadas del mercado.

6. TRANSPARENCIA, DERECHOS Y EXPLICABILIDAD

Aunque el anteproyecto recoge principios como transparencia y supervisión humana, se considera insuficiente en términos de derechos explícitos.

Se propone incorporar:

- Derecho a información clara.
- Derecho a revisión humana en función del grado de impacto/ riesgo o criticidad.
- Derecho a retirar consentimiento y a conocer que elementos o áreas de la administración usan cada dato como ya se hace en la normativa de algunos países (UK)
- Derecho a corregir errores automatizados.

Asimismo, se advierte que la transparencia técnica (registro IA) no garantiza comprensibilidad ciudadana.

Se recomienda crear fichas informativas en lenguaje sencillo para cada sistema IA.

7. SUPERVISIÓN HUMANA Y MOTIVACIÓN DE RESOLUCIONES

Preocupación operativa relevante:

- Exigir excesivo detalle técnico en cada resolución administrativa puede ser inviable.
- Debe separarse lo que figura en la resolución de lo que queda en expediente técnico auditable.

Se cuestiona si la intervención opcional de la Oficina Técnica puede dilatar procedimientos.



8. SEGURIDAD Y CIBERSEGURIDAD

Se reconoce alineación con ENS. Se manifiestan importantes dudas respecto a:

- Confluir en la agencia la **capacidad de definición de la estrategia de seguridad, regulación control y supervisión de organismos públicos y a la vez la responsabilidad de ejecución** en alguno de ellos de acuerdo con las disposiciones finales.
- La capacidad de la Agencia para asumir, con el modelo y dotación actuales, las responsabilidades que se le incorporan.

Se propone reforzar:

- **Separar la definición y supervisión de la ejecución.**
- Seguridad específica para sistemas IA.
- Protección frente a ataques a modelos y manipulación de datos.
- Cláusulas contractuales tipo para proveedores.
- Monitorización de riesgos algorítmicos.

9. IDENTIDAD DIGITAL Y EIDAS2

Se detecta ausencia de referencia explícita al Reglamento eIDAS2 y a la futura EUDI Wallet.

Se recomienda preparar hoja de ruta hacia credenciales verificables y gestión granular del consentimiento.

10. CUENTA DIGITAL Y CANALES

Se detectan incoherencias conceptuales en la definición de “Cuenta Digital”.

Se recomienda:

- Claridad conceptual.
 - Gestión de consentimiento granular.
 - Panel de transparencia de uso de datos.
 - Gobernanza de canales.
 - Clarificar carácter no formal de canales informales.
-



11. INCLUSIÓN DIGITAL, EQUIDAD Y AUDITORÍA

Aunque se mencionan principios de no discriminación, se pide mayor concreción operativa.

Se recomienda:

- Auditorías independientes y recurrentes de IA.
- Registro de entidades auditoras acreditadas.
- Diagnóstico de inclusión digital previo a despliegue.
- Garantía explícita de atención presencial en función de criticidad.

12. Principales debilidades detectadas

También de forma más general pueden señalarse algunas debilidades o aspectos de mejora relevantes.

3.1. Limitada ambición transformadora

- La ley **no redefine procesos**, solo habilita tecnología.
- Se centra en “usar IA” más que en **reimaginar la Administración**.
- Limitada visión de **Administración proactiva, predictiva y centrada en el ciudadano**.
- Ausencia de KPIs claros de transformación u objetivos de transformación de las Administración identificables.

3.2. Insuficiente desarrollo operativo si bien pueden desarrollarse a través de reglamentos.

Las empresas recomiendan el uso de la Ley allí donde se pueda por ser una norma de mayor impacto que los reglamentos.

- Muchos principios sin:
 - Indicadores.
 - Obligaciones concretas.
 - Mecanismos de rendición de cuentas.
- No se define:
 - Quién responde por errores algorítmicos.
 - Cómo se auditan los sistemas en la práctica.

3.3. Talento y capacidades



- No aborda de forma estructural:
 - Atracción de talento digital.
 - Nuevos perfiles profesionales.
 - Formación masiva de empleados públicos.
- Riesgo de **dependencia excesiva de proveedores externos**.

3.4. Débil enfoque económico y de impacto

- No se establecen:
 - KPIs de ahorro, eficiencia o mejora del servicio.
 - Evaluaciones coste-beneficio.
- La IA como gasto tecnológico, no como **palanca de productividad pública**.

13. Oportunidades no desarrolladas en profundidad

- La ley focaliza en poner la digitalización y la IA al servicio de mejorar los servicios al ciudadano pero no profundiza tanto en utilizarla para aumentar la eficiencia y la eficacia de la propia administración:
 - Prevención del fraude.
 - Anticipación de demandas ciudadanas.
 - Gestión predictiva de servicios públicos (sanidad, empleo, movilidad, servicios sociales).
 - Sinergias y ahorros de gasto.
- Integración con:
 - Compra pública innovadora.
 - Sandboxes regulatorios para facilitar la transformación de la administración y no solo para dinamizar la industria de la innovación
 - Colaboración universidad–empresa.
- Posicionar a la Comunidad como **laboratorio europeo de IA pública**, no solo como usuaria.



14. CONCLUSIÓN GENERAL

El consenso del Consejo Asesor considera claramente que la orientación del Anteproyecto es acertada, el momento es oportuno y la Comunidad de Madrid dispone de una oportunidad real para situarse en la vanguardia europea en materia de gobernanza pública de la Inteligencia Artificial.

La iniciativa es sólida en su planteamiento institucional y coherente con el marco europeo.

El texto construye una arquitectura organizativa ambiciosa, incorpora garantías relevantes y se alinea conceptualmente con el AI Act.

No obstante, en su redacción actual, el Anteproyecto presenta un enfoque predominantemente normativo y organizativo, orientado a establecer estructuras, controles y principios de supervisión.

Para situar a la Comunidad de Madrid en el grupo de territorios que no solo regulan la IA sino que transforman su Administración mediante ella, sería necesario reforzar de manera explícita los elementos de ejecución, medición de impacto y rediseño de procesos.

La Comunidad de Madrid no debe limitarse a regular la IA. Debe aspirar a gobernar con IA como palanca de transformación de la administración.

Para ello, el texto podría evolucionar desde un modelo habilitante y garantista hacia un modelo plenamente operativo, medible y orientado a resultados. Esto implica profundizar en:

- Reforzar la precisión conceptual y evitar cualquier duplicidad normativa con el marco europeo.
- Consolidar una gobernanza ejecutiva clara, con responsabilidades inequívocas y sin solapamientos.
- Establecer procedimientos integrados que eviten cuellos de botella administrativos.
- Clarificar el régimen de responsabilidad ante errores o incidencias algorítmicas.
- Dotar de medios, talento y capacidades suficientes a las estructuras creadas por la ley.

En este contexto, resulta relevante la recomendación de garantizar la separación efectiva de funciones en materia de ciberseguridad y supervisión tecnológica. La concentración en un mismo órgano de competencias de definición estratégica, supervisión, control y ejecución operativa podría generar riesgos de conflicto de funciones, autocontrol y pérdida de independencia efectiva.

Asimismo, la Ley debe incorporar de manera expresa el principio de evaluación y



rendición de cuentas sobre el impacto real de la Inteligencia Artificial en la transformación administrativa.

No basta con habilitar el uso de tecnologías avanzadas; es necesario medir su efecto.

Por ello, el texto legal podría establecer el mandato explícito de evaluar el impacto de los sistemas de IA en términos de eficiencia, productividad, reducción de tiempos de tramitación, calidad del servicio, ahorro de recursos públicos y disminución de cargas administrativas esperados.

La definición técnica de indicadores podrá desarrollarse reglamentariamente, pero la obligación de medir, evaluar y publicar resultados debería quedar recogida desde el propio rango legal, evitando que la transformación quede en el plano meramente declarativo.

La norma puede proyectar, además, una visión ambiciosa de Administración pública: una Administración proactiva, predictiva, centrada en el ciudadano y apoyada en datos para anticipar necesidades, prevenir fraude, optimizar recursos y mejorar la toma de decisiones.

Europa ya se divide entre territorios que regulan la IA y territorios que gobiernan con IA.

La LADIA ofrece a la Comunidad de Madrid la posibilidad de situarse en este segundo grupo.

Con los ajustes señalados, el Anteproyecto puede convertirse no solo en una norma jurídicamente robusta y alineada con el AI Act, sino en un verdadero marco de transformación institucional, competitividad económica y liderazgo público en la nueva era digital que supere la actual regulación existente en Europa.



Anexo1. Recomendaciones detalladas

A. Coherencia normativa con AI Act y “no duplicación”

Problema detectado: riesgo de “marco paralelo” autonómico (registros, evaluaciones, obligaciones ya cubiertas por AI Act) y fragmentación regulatoria.

Recomendaciones concretas

- **Cláusula de remisión fuerte:** cuando el anteproyecto trate materias “sustantivas” de IA (clasificación de riesgo, obligaciones de proveedores/desplegadores, documentación, etc.), **remitir expresamente** al AI Act y evitar reescrituras.
- **Arquitectura “organización + procedimiento”:** centrar la ley autonómica en *cómo* la Administración madrileña decide, aprueba, despliega, audita y responde ante incidentes; no en replicar requisitos técnicos del AI Act.
- **Un solo registro operativo:** si hay Registro autonómico, que sea “**ventana administrativa**” para inventario y transparencia interna/ciudadana, pero **sin crear** obligaciones adicionales de evaluación técnica duplicada.

B. Gobernanza IA real (RACI, circuito único, portfolio y “stop button”)

Problema detectado: riesgo de solapamientos (Oficina Técnica / Ética / Dato / Ciber) y circuitos secuenciales lentos.

Recomendaciones concretas

- **RACI interorgánico por norma o reglamento:** responsabilidades claras entre Oficina Técnica IA, gobierno del dato, ciberseguridad y comité ético (quién decide, quién informa, quién audita, quién aprueba).
- **“Circuito único” de aprobación:** expediente estándar que integre, en paralelo, revisión de dato + seguridad + ética + legal (evitar retrabajos).
- **Gestión del portfolio IA:** priorización, cadencia, criterios de escalado y retirada (qué se aprueba/qué se mantiene/qué se apaga).
- **Gestión de incidencias IA:** procedimiento de incidentes (técnicos/éticos/seguridad) con criterios de **parada/rollback** y trazabilidad de decisiones.

C. Dato: “compartición por defecto” con límites claros (secreto empresarial y base jurídica)



Problema detectado: la compartición obligatoria puede invadir datos aportados por privados y comprometer secreto empresarial/IP/confidencialidad.

Recomendaciones concretas

- **Separar tipologías:** datos y algoritmo y modelos institucionales vs. los aportados por empresas en relaciones contractuales/procedimentales.
 - **Exclusiones explícitas:** incorporar salvaguarda legal para secreto empresarial, IP, confidencialidad contractual y normativa sectorial.
 - **“Data sharing agreements”:** plantillas de acuerdos de compartición, linaje, control de finalidad, retención y auditoría.
 - **Data governance serio:** roles (owner/steward), catálogo, linaje, “quality gates” y trazabilidad.
-

D. Interoperabilidad y ecosistema: APIs abiertas, neutralidad tecnológica y “no duplicar el mercado”

Problema detectado: si la Administración crea herramientas para empresas sin integrarse con software real, genera duplicidades/carga.

Recomendaciones concretas

- **Obligación de interoperabilidad:** APIs públicas, estándares abiertos y neutralidad tecnológica para integrar soluciones privadas con sistemas públicos.
 - **Gobernanza API:** catálogo, versionado, SLAs, eventos y acuerdos tipo.
 - **Diseño “complementario”:** herramientas públicas para empresas deben integrarse con ERPs/gestión existentes y evitar duplicidades funcionales.
-

E. Transparencia y derechos: pasar de “registro técnico” a confianza ciudadana

Problema detectado: transparencia técnico-administrativa no garantiza comprensibilidad; falta un bloque claro de derechos.

Recomendaciones concretas

- **Carta de derechos frente a IA:** información clara, revisión humana, retirada de consentimiento sin perjuicio, corrección de errores automatizados, etc.
- **Ficha pública por sistema** en lenguaje sencillo: para qué sirve, efectos, derechos, reclamación/revisión.
- **Transparencia escalonada:** lo mínimo en la resolución; lo técnico en expediente auditable con acceso graduado (para evitar tensiones con seguridad y confidencialidad).



F. Resoluciones administrativas: motivación defendible sin pedir “ingeniería” en cada acto

Problema detectado: exigir detalle técnico excesivo en cada resolución es difícil y puede chocar con seguridad/confidencialidad.

Recomendaciones concretas

- **Separar dos planos:**
 1. **Resolución:** explicación suficiente para comprender/impugnar/controlar.
 2. **Expediente técnico:** documentación completa, auditable, con control de acceso. No público
- **Evitar cuellos de botella:** si el informe de Oficina Técnica es “opcional” pero en la práctica se vuelve imprescindible, puede dilatar. Ajustar y detallar cuándo aplica.

G. Seguridad/ENS + seguridad específica IA (“AI security de verdad”)

Problema detectado: ENS está bien, pero falta aterrizar amenazas específicas a modelos/datos y obligaciones para terceros.

Recomendaciones concretas

- **Requisitos IA-security** en desarrollo reglamentario: ataques a modelos, envenenamiento de datos, manipulación de logs, etc.
- **Cláusulas contractuales tipo** para proveedores: auditoría, trazabilidad, continuidad, responsabilidades, datos, etc.
- **Comité de riesgo digital/IA:** integrar ciber + dato + IA para priorizar mitigaciones e incidentes.

H. Identidad digital y EUDI Wallet (eIDAS2): preparar la hoja de ruta

Problema detectado: falta referencia clara a eIDAS2/EUDI Wallet pese a su impacto próximo.

Recomendaciones concretas

- **Incluir eIDAS2/EUDI Wallet** y plan de adopción, además de credenciales verificables y consentimiento granular.



I. Cuenta Digital y canales informales: coherencia, trazabilidad y “escalado a canal formal”

Problema detectado: incoherencias internas del concepto “Cuenta Digital” y riesgo de que canales informales se confundan con acto administrativo.

Recomendaciones concretas

- **Definición única y consistente** de Cuenta Digital (área personal vs. evolución de sede).
- **Guardarrailes:** aviso explícito en canales informales + reglas de escalado a canal autenticado cuando haya efecto jurídico.
- **Gobierno de canales:** inventario, responsables, SLA, auditoría y retención de trazas también en “informales”.

J. Inclusión digital y equidad: de “principios” a mecanismos verificables

Problema detectado: hay muchas menciones a no discriminación, accesibilidad, sesgos, pero poca operativa.

Recomendaciones concretas

- **Auditorías independientes recurrentes** y resultados vinculantes para órganos responsables.
 - **Registro de entidades auditoras acreditadas.**
 - **Diagnóstico de inclusión digital** antes de aprobar el despliegue.
 - **Atención presencial garantizada** para colectivos no digitalizados.
-



CONSEJO ASESOR
DE TRANSFORMACIÓN DIGITAL