Madrid, 26 de febrero de 2026

Informe de adecuación sobre el Borrador del Anteproyecto de Ley de la Administración Digital e Inteligencia Artificial de la Comunidad de Madrid

1. Objeto y alcance de la evaluación

El presente informe tiene por objeto evaluar de forma integral la adecuación normativa, técnica y estratégica del Borrador del Anteproyecto de Ley de Administración Digital e Inteligencia Artificial de la Comunidad de Madrid (LADIA). La evaluación abarca la totalidad del articulado, definiciones, estructuras de gobernanza, disposiciones adicionales y procedimientos operativos previstos en la ley, con especial atención a su interacción con:

- **Esquema Nacional de Seguridad (ENS),** aprobado por Real Decreto 311/2022, de 3 de mayo, como marco de referencia obligatorio para las administraciones públicas españolas en materia de seguridad de la información y ciberseguridad.
- **Reglamento (UE) 2024/1689 de Inteligencia Artificial (AI Act),** en lo relativo a los requisitos de ciberseguridad, robustez técnica, seguridad de los sistemas de alto riesgo y protección frente a ciberataques, manipulaciones y accesos no autorizados.
- **Directiva (UE) 2022/2555 (NIS2),** sobre medidas de ciberseguridad común en toda la Unión, aplicable a entidades esenciales e importantes del sector público digital, y cuya transposición al ordenamiento español se encuentra en fase de desarrollo normativo.
- **Estándares internacionales de seguridad de la información:** ISO/IEC 27001:2022 (Sistemas de Gestión de Seguridad de la Información), ISO/IEC 27002:2022 (Controles de seguridad), ISO/IEC 27005:2022 (Gestión de riesgos de seguridad), ISO/IEC 42001:2023 (Sistemas de Gestión de Inteligencia Artificial, en lo relativo a seguridad de sistemas de IA).
- **Ley 14/2023, de 20 de diciembre**, por la que se crea la Agencia de Ciberseguridad de la Comunidad de Madrid, que establece el marco institucional de gobernanza de la ciberseguridad autonómica y determina las competencias y funciones del CSIRT regional.
- **Marco Nacional de Ciberseguridad** y normativa estatal aplicable: Ley 36/2015 de Seguridad Nacional, Plan Nacional de Ciberseguridad, CCN-STIC (guías técnicas del Centro Criptológico Nacional).

Asimismo, la evaluación analiza **la coherencia interna** del anteproyecto en la distribución de responsabilidades en materia de ciberseguridad entre los distintos órganos previstos (Oficina Técnica de Impulso de la Inteligencia Artificial, Consejo para la Inteligencia Artificial, Comité de Ética, órganos competentes por razón de la materia) y la **Agencia de Ciberseguridad de la Comunidad de Madrid**, así como la suficiencia de las medidas previstas para garantizar un nivel elevado y homogéneo de ciberseguridad en todo el sector público autonómico.

El propósito último es **identificar brechas normativas, diagnosticar insuficiencias técnicas y organizativas, y formular recomendaciones** que permitan a la Comunidad de Madrid desplegar una infraestructura digital segura, resiliente y conforme con las obligaciones europeas y nacionales en materia de ciberseguridad, integrando de forma efectiva el papel de la Agencia de Ciberseguridad como ente rector y coordinador de la seguridad digital autonómica.

2. Consideraciones generales del análisis

La evaluación se ha realizado siguiendo una metodología homogénea, rigurosa y replicable para todas las materias, estructurada en tres fases analíticas internas: (1) **extracción y parafraseo de extractos relevantes**; (2) **juicio comparado con el marco normativo y técnico aplicable**; y (3) **medidas de adecuación normativa y organizativa**. Este enfoque se aplica sistemáticamente en las subsecciones del punto 3 del informe.

En primer lugar, para cada epígrafe temático se procede a una lectura directa del articulado de la LADIA y se extraen y parafrasean los elementos más relevantes, a fin de condensar su contenido y permitir la **trazabilidad entre el texto legal y el análisis técnico-jurídico**. Este parafraseo sirve de base objetiva para el contraste posterior.

En segundo lugar, a partir de dicha extracción se **evalúa el grado de alineamiento** del anteproyecto con los requisitos del ENS, el AI Act (en materia de ciberseguridad de sistemas de IA), la Directiva NIS2, los estándares ISO 27001/27002/27005, la normativa de la Agencia de Ciberseguridad y las mejores prácticas internacionales. Esta fase permite **identificar fortalezas, debilidades, omisiones, ambigüedades y riesgos de incumplimiento normativo o técnico** que comprometan la seguridad, disponibilidad, integridad, confidencialidad y resiliencia de las infraestructuras y servicios digitales.

Finalmente, para cada materia se formulan **medidas concretas de adecuación**: recomendaciones de redacción normativa, adiciones procedimentales, requisitos técnicos, controles de seguridad, mecanismos de supervisión y auditoría, coordinación con la Agencia de Ciberseguridad, gestión de incidentes, continuidad de negocio, formación en ciberseguridad y criterios de gobernanza. Estas propuestas están diseñadas para facilitar la aplicación práctica de la LADIA y asegurar su plena compatibilidad con las obligaciones europeas, nacionales y autonómicas, garantizando la seguridad jurídica, la claridad organizativa y la efectividad del marco autonómico de ciberseguridad.

A lo largo del análisis del articulado se ha constatado que el texto de la LADIA:

1. **Reconoce de forma explícita la importancia de la ciberseguridad** como elemento transversal de la administración digital, incluyendo un **Título III** específico dedicado a la seguridad de la infraestructura digital.

2. **Establece obligaciones genéricas de ciberseguridad** alineadas conceptualmente con los principios del ENS (seguridad desde el diseño, medidas proporcionales al riesgo, protección de datos).

3. **Se identifican deficiencias en la especificación técnica y procedimental** en diversas áreas clave. En determinados casos, no se menciona de manera explícita el ENS como marco normativo obligatorio, ni se detallan las categorías de seguridad. Además, se omiten los procedimientos para la gestión de incidentes, no se establecen obligaciones de notificación, y faltan requisitos relativos a auditoría y certificación.

4. **No articula de forma expresa la coordinación con la Agencia de Ciberseguridad** en la implantación, supervisión y respuesta ante incidentes de seguridad, pese a ser el ente autonómico competente creado por Ley 14/2023.

5. **Se observan omisiones en cuanto a la ciberseguridad de los sistemas de IA**, al no incorporar los requisitos específicos establecidos por el AI Act relativos a la robustez, resistencia frente a ciberataques, seguridad durante todo el ciclo de vida, así como la protección de modelos y datos de entrenamiento.

6. **No incorpora mecanismos de supervisión continua, auditoría externa obligatoria ni régimen sancionador** en materia de incumplimiento de obligaciones de ciberseguridad.

7. **Requiere mayor especificidad operativa, terminológica y procedimental** para asegurar aplicabilidad efectiva, homogeneidad en el nivel de protección y alineamiento pleno con ENS, NIS2 y AI Act

Estas consideraciones se desarrollan en los apartados siguientes, incluyendo referencias literales del anteproyecto y propuestas concretas de modificación

A efectos de este informe, solo se consideran **referencias suficientes** al Esquema Nacional de Seguridad (ENS) aquellas que utilicen fórmulas imperativas tales como “se ajustarán a”, “de conformidad con” o “de aplicación obligatoria”. Por el contrario, las expresiones “teniendo en cuenta”, “se considerarán” u otras fórmulas similares se valoran como **insuficientes**, al no garantizar por sí mismas la plena sujeción de los sistemas y servicios al marco obligatorio del ENS

3. Evaluación por títulos y disposiciones

3.1 Título Preliminar – Capítulo I - DISPOSICIONES GENERALES

Extractos LADIA

- **p. 17 — Art. 5.b**

- *"Garantizarán un elevado nivel de ciberseguridad de los servicios públicos digitales mediante un enfoque reforzado con la adopción de medidas adaptadas en cada momento que aseguren desde el diseño e implantación inicial de herramientas y soluciones digitales la salvaguarda de los derechos de los sujetos interesados."*

- **p. 17-18 — Art. 5.d**
  - *"Garantizarán la privacidad y la seguridad de todos los datos, incluidos los datos neuronales y biométricos, a los que tengan acceso a través de los servicios públicos digitales mediante el establecimiento sistemático de medidas de protección de la privacidad desde el diseño y por defecto en cualquier plan o actuación de fomento digital."*

Conclusión

El anteproyecto **incorpora correctamente el principio de seguridad desde el diseño** (*security by design*), alineado conceptualmente con el **art. 10 del ENS** y con los principios de *privacy by design* del RGPD. La referencia a "medidas adaptadas en cada momento" sugiere proporcionalidad al riesgo, coherente con el enfoque del ENS.

No obstante, la obligación está definida de manera general y no se vincula expresamente con un Sistema de Gestión de Seguridad de la Información (SGSI) formal. No hay certeza de que exista una política de seguridad debidamente aprobada, un análisis de riesgos documentado, una declaración de aplicabilidad, controles implementados ni auditorías internas regulares. Además, no se hace referencia a la coordinación con la Agencia de Ciberseguridad, que es la entidad autonómica responsable de establecer y supervisar la implementación de las políticas públicas en este ámbito.

Medidas de adecuación

La ley debería incorporar un artículo específico que establezca:

- Que la Administración de la Comunidad de Madrid contará con un **Sistema de Gestión de Seguridad de la Información** alineado con el ENS de aplicación a todo el sector público autonómico.
- Que dicho sistema incluirá, como mínimo: una **política de seguridad aprobada** por el órgano competente, un **análisis de riesgos documentado**, una **declaración de aplicabilidad** de controles, un plan de tratamiento de riesgos y **auditorías internas periódicas.**
- Que la **Agencia de Ciberseguridad de la Comunidad de Madrid** será el órgano responsable de coordinar el diseño, implantación, supervisión y mejora continua de este sistema de gestión, en el ámbito de sus competencias legales.

Con estas previsiones, la ley demostraría que el modelo madrileño de administración digital opera con las garantías mínimas exigidas por el ENS y por las buenas prácticas internacionales de gestión de la seguridad.

3.2 Título I – Capítulo I

Extractos LADIA

- **p. 27 — Art. 19.3**
    - *"Se habilitarán recursos y dispositivos en las sedes administrativas para facilitar el acceso digital, y se dispondrán canales de atención, orientación y asistencia al usuario, incluyendo aquellos que puedan basarse en inteligencia artificial como los chatbots o agentes de inteligencia artificial. Igualmente, se establecerán mecanismos que aseguren la confidencialidad, seguridad e interoperabilidad de estos canales, así como la continuidad del servicio ante situaciones de indisponibilidad tecnológica."*
- **p. 27 — Art. 19.4**
    - *"Las plataformas o canales de servicios públicos digitales se ajustarán a los requisitos de seguridad e interoperabilidad establecidos en el Esquema Nacional de Seguridad y el Esquema Nacional de Interoperabilidad, sin que puedan existir restricciones o discriminaciones en el acceso de las personas y entidades interesadas a los servicios públicos digitales."*

Conclusión

El artículo 19.4 hace una referencia adecuada tanto al ENS como al ENI, indicando que las plataformas o canales digitales de servicios públicos deben cumplir con sus requisitos de seguridad e interoperabilidad; esto supone una obligación estricta de adherirse a ambos estándares en este contexto. Además, la cita sobre la "continuidad del servicio ante situaciones de indisponibilidad tecnológica" (artículo 19.3) se alinea con el criterio de disponibilidad del ENS.

No obstante, estas previsiones son parciales y se centran exclusivamente en los canales y plataformas de acceso. El título no establece obligaciones expresas de **categorización ENS, análisis de riesgos, planes de continuidad ni pruebas periódicas** para los servicios digitales esenciales, ni vincula estas obligaciones con la Agencia de Ciberseguridad. La falta de desarrollo operativo limita el alcance real de la referencia al ENS

Medidas de adecuación

La ley debería:

- Establecer la obligación de categorizar los sistemas que soportan servicios públicos digitales conforme al ENS, realizar un análisis de riesgos y aplicar las medidas de seguridad correspondientes a su categoría.
- Incorporar la exigencia de planes formales de continuidad y recuperación para los servicios digitales esenciales, con objetivos de tiempo y punto de recuperación (RTO/RPO) documentados, probados regularmente y revisados tras incidentes o cambios relevantes.

- Atribuir a la Agencia de Ciberseguridad de la Comunidad de Madrid la función de supervisar la adecuada aplicación del ENS a estos servicios, así como la revisión periódica de los planes de continuidad y sus pruebas.

3.2 Título I – Capítulo II

Extractos LADIA

- **p. 29 — Art. 20 (Principios generales en el uso, desarrollo y despliegue de sistemas de inteligencia artificial)**
    - *"**Seguridad**: supone proteger los datos, procesos y resultados de agentes externos, eventos adversos e información errónea. Para ello, es necesario aplicar prácticas sólidas y resistentes que incluyan el uso de protocolos de ciberseguridad, cifrado, controles de acceso y auditorías periódicas. Un sistema seguro debe ser resistente a las vulnerabilidades y responder eficazmente a posibles ataques o interrupciones, garantizando la continuidad y fiabilidad de su funcionamiento."*
- **p. 31 — Art. 21.4**
    - *"El tratamiento de los datos personales exigirá la adopción de las medidas de seguridad necesarias conforme a lo dispuesto en el Esquema Nacional de Seguridad en el ámbito de la administración electrónica y en la normativa en materia de protección de datos de carácter personal."*

Conclusión

El artículo 20 incorpora de forma adecuada la noción de seguridad aplicada a los sistemas de inteligencia artificial, al mencionar expresamente protocolos de ciberseguridad, cifrado, controles de acceso y auditorías periódicas. Esta formulación es coherente con el espíritu del artículo 15 del AI Act (ciberseguridad y robustez) y recoge buenas prácticas internacionales.

El artículo 21.4 establece una referencia explícita al ENS en relación con el tratamiento de datos personales en el contexto de la administración electrónica, lo que representa un fundamento normativo relevante. No obstante, el anteproyecto no incorpora los requisitos materiales obligatorios previstos en el AI Act para sistemas de alto riesgo, como la gestión de riesgos, robustez, resistencia frente a ciberataques, seguridad durante todo el ciclo de vida o trazabilidad mejorada; tampoco los integra dentro de un sistema específico de gestión de riesgos de IA. Se observa que el marco de IA aún no contempla formalmente la identificación, análisis y tratamiento de riesgos de seguridad propios de la IA, debidamente articulados con el SGSI general.

Medidas de adecuación

La ley debería incorporar un artículo específico sobre **"Ciberseguridad de los sistemas de inteligencia artificial"**, encuadrado en el Título I o, en su defecto, en el Título III, que establezca al menos:

- La obligación de que todo sistema de IA utilizado por el sector público autonómico se someta a un **análisis de riesgos de ciberseguridad previo al despliegue**, actualizado periódicamente, identificando amenazas específicas (ciberataques al modelo, envenenamiento de datos, manipulación de salidas, accesos no autorizados, pérdida de trazabilidad, etc.).
- La exigencia de que los sistemas de IA que traten datos personales o soporten servicios esenciales se integren en el **Sistema de Gestión de Seguridad de la Información** de la Comunidad de Madrid, de conformidad con el ENS.
- La fijación de **requisitos mínimos de seguridad** para los sistemas de IA de alto impacto o alto riesgo, alineados con el artículo 15 del AI Act: pruebas de robustez, mecanismos de detección de anomalías, registros de actividad (logging), monitorización continua y planes de respuesta ante incidentes.
- La obligación de que **los proveedores y terceros** que suministren sistemas de IA a la Administración acrediten un nivel adecuado de madurez en ciberseguridad (cumplimiento del ENS cuando proceda, certificaciones ISO/IEC 27001 u otras equivalentes) y acepten contractualmente la notificación y gestión conjunta de incidentes.
- La incorporación de una **obligación expresa de notificación** de incidentes de ciberseguridad asociados a sistemas de IA al CSIRT competente de la Comunidad de Madrid y a la Agencia de Ciberseguridad, con plazos, canales y contenidos mínimos, en coherencia con el ENS y con la futura trasposición de NIS2.
- La exigencia de que los sistemas de IA que soporten servicios públicos esenciales o funciones críticas cuenten con **medidas reforzadas de continuidad** y recuperación, incluyendo copias de seguridad, planes de contingencia, pruebas periódicas y capacidad de degradación controlada o desconexión segura en caso de incidente grave.

Esta previsión permitiría que el principio general de seguridad del artículo 20 se traduzca en obligaciones técnicas, organizativas y de gestión del riesgo plenamente alineadas con el ENS, el AI Act y los sistemas de gestión de seguridad e IA

3.3 Título II — Capítulo II

Extractos LADIA

- **pp. 39–40 — Art. 32 (Sistemas de firma electrónica)**
    - *"La Comunidad de Madrid admitirá, en sus relaciones por medios electrónicos, sistemas de firma electrónica que sean conformes a lo establecido en la normativa vigente sobre firma electrónica garanticen la identificación de las personas interesadas y, en su caso, la autenticidad e integridad de los documentos electrónicos."*
- **pp. 40–41 — Art. 35 (Sistema único de registro)**
    - *"[...]Estos registros deberán ser plenamente interoperables, estar interconectados con el Registro Electrónico General de la Comunidad de Madrid y cumplir con las garantías y medidas de seguridad contempladas en la legislación en materia de protección de datos de carácter personal y de seguridad de la información."*
- **pp. 42–43 — Art. 38.3 (Archivo electrónico único)**
    - *"La gestión del archivo electrónico único garantizará la autenticidad, conservación, integridad, confidencialidad, disponibilidad y cadena de custodia de los expedientes y documentos almacenados, así como su acceso, en las condiciones exigidas por el Esquema Nacional de Interoperabilidad y el Esquema Nacional de Seguridad."*

Conclusión

El Título II incorpora referencias parciales a la seguridad de la información en relación con firma electrónica, registros y archivo. El artículo 32 se remite correctamente a la normativa de firma electrónica para garantizar identificación, autenticidad e integridad de los documentos; el artículo 38.3 es el más completo al mencionar expresamente ENS y ENI y al enumerar los atributos de autenticidad, conservación, integridad, confidencialidad, disponibilidad y cadena de custodia, en línea con las dimensiones de seguridad del ENS y los requisitos del ENI.

Sin embargo, la referencia del artículo 35 a "las garantías y medidas de seguridad contempladas en la legislación en materia de protección de datos de carácter personal y de seguridad de la información" es excesivamente genérica y no menciona de forma expresa el ENS, lo que genera ambigüedad sobre el estándar mínimo exigible. Además, el título no establece la obligación de categorización ENS, análisis de riesgos ni auditorías periódicas para estos sistemas clave (registros, identificación, archivo), ni vincula su supervisión con la Agencia de Ciberseguridad.

Medidas de adecuación

La ley debería:

- Modificar el artículo 35 para que remita de forma expresa y directa al ENS como marco de referencia mínimo para las garantías y medidas de seguridad de los registros electrónicos, evitando remisiones genéricas a la "legislación en materia de seguridad de la información".

- Establecer que los sistemas regulados en el Título II (identificación, firma, registro y archivo electrónico) se someterán a **categorización formal ENS, análisis de riesgos y auditorías periódicas,** de acuerdo con el RD 311/2022.

- Atribuir a la **Agencia de Ciberseguridad de la Comunidad de Madrid** la supervisión del cumplimiento de estas obligaciones, incluyendo la coordinación con la Agencia responsable de la administración digital en lo que respecta a diseño y operación de estos sistemas.

3.4 Título III — Seguridad de la infraestructura digital

3.4.1 Art. 39 — Seguridad de la infraestructura digital

Extractos LADIA

- **p. 43 — Art. 39.1**
  - *"La Comunidad de Madrid será responsable de definir y velar por la ejecución de políticas públicas en materia de ciberseguridad, incluyendo las relativas a capacitación y de concienciación al respecto, de administrar y controlar las infraestructuras digitales que den soporte a los servicios regulados en la presente ley, garantizando su seguridad y la protección de los datos involucrados en ejercicio de las competencias y fines públicos, así como de gestionar las respuestas ante posibles incidentes que puedan producirse en este ámbito, atendiendo a las mejores prácticas y estándares que correspondan en este ámbito a nivel internacional."*
- **p. 43 — Art. 39.2**
  - *"A estos efectos se considerarán normas como la normativa aplicable relativa al Esquema Nacional de Seguridad, o cualquier otra que pueda aplicar a la Comunidad de Madrid en materia de seguridad de la información o protección de los datos tratados por la misma. Del mismo modo, se prestará especial atención al cumplimiento de la normativa protectora de datos personales que aplique en la Comunidad."*

Conclusión

El artículo 39 configura un marco general de responsabilidad de la Comunidad de Madrid en materia de ciberseguridad de infraestructuras digitales, integrando tres funciones clave: definición y ejecución de políticas públicas de ciberseguridad, administración y control de infraestructuras digitales y gestión de respuestas ante incidentes. Esta aproximación es conceptualmente coherente con el rol que la Ley 14/2023 atribuye a la Agencia de Ciberseguridad.

No obstante, el precepto presenta carencias: la referencia al ENS en el apartado 2 es meramente potestativa ("se considerarán normas como"), cuando el ENS es de aplicación obligatoria para todas las Administraciones Públicas (art. 2 RD 311/2022). El artículo atribuye la responsabilidad genérica a "la Comunidad de Madrid" sin identificar el órgano competente, omitiendo la referencia expresa a la Agencia de Ciberseguridad de la Comunidad de Madrid. Además, la gestión de incidentes se formula sin definir categorías, plazos, umbrales de notificación, canales ni responsables, lo que resulta incompatible con las exigencias del ENS y con la futura trasposición de NIS2.

Medidas de adecuación

La ley debería:

- Sustituir la fórmula "se considerarán normas como la normativa aplicable relativa al Esquema Nacional de Seguridad" por "se aplicará con carácter obligatorio el Esquema Nacional de Seguridad y, en lo que resulte de aplicación, la normativa de trasposición de la Directiva NIS2".

- Identificar expresamente a la Agencia de Ciberseguridad de la Comunidad de Madrid como órgano responsable de la coordinación, supervisión y ejecución de las políticas de ciberseguridad en el ámbito de las infraestructuras digitales reguladas en este título.

- Incluir un apartado específico que regule la gestión de incidentes de ciberseguridad, fijando categorías de incidentes, plazos máximos de notificación al CSIRT regional (por ejemplo, 72 horas para incidentes significativos), contenidos mínimos de la notificación, canales y mecanismos de coordinación con el CCN-CERT.

- Establecer la obligación de realizar, al menos **cada dos años**, un **análisis de riesgos formal** de las infraestructuras digitales del sector público autonómico conforme a la metodología ENS o equivalente, cuyos resultados alimenten la política de seguridad del artículo 40.

3.4.2 Art. 40 — Política de Seguridad y Escudo Digital

Extractos LADIA

- **pp. 43–44 — Art. 40.1**
  - *"La Comunidad de Madrid establecerá la política de seguridad de la información de aplicación general en el sector público autonómico, teniendo en cuenta la normativa vigente en materia de seguridad de las redes y sistemas de información por relación al Esquema Nacional de Seguridad, entre otra posible normativa aplicable."*

- **pp. 43–44 — Art. 40.2**
  - *"La política de seguridad establece los principios rectores y la estructura organizativa en materia de seguridad de la información. Asimismo, define las medidas de seguridad de carácter organizativo, físico y lógico necesarias para garantizar la integridad, autenticidad, confidencialidad, disponibilidad, trazabilidad, calidad, protección, recuperación y conservación de la información [...] en función de los riesgos identificados y de los plazos de conservación de la información. Estas medidas serán de obligado cumplimiento para toda la infraestructura digital del sector público autonómico, así como para las personas y entidades interesadas que interactúen con dicha infraestructura digital en el marco de procedimientos administrativos o servicios digitales. Se prestará especial atención a la iniciativa de Escudo Digital de la Comunidad de Madrid para proteger a la región de ataques y amenazas cibernéticas y, en particular, para proteger la prestación y la continuidad de los servicios públicos digitales."*

- **pp. 43–44 — Art. 40.3**
  - *"En desarrollo de la política de seguridad, se adoptarán medidas específicas en [...]"*

Conclusión

El artículo 40 es el precepto conceptualmente más avanzado del Título III en materia de seguridad de la información. La política de seguridad incorpora los cinco atributos clásicos del ENS (integridad, autenticidad, confidencialidad, disponibilidad y trazabilidad), así como calidad, protección, recuperación y conservación, establece su carácter obligatorio para toda la infraestructura digital del sector público autonómico y menciona el Escudo Digital como instrumento específico de protección regional. La referencia a la capacitación como medida de desarrollo es coherente con una aproximación integral.

Sin embargo, la redacción actual sigue siendo insuficiente para garantizar plena conformidad con el ENS: la referencia al Esquema Nacional de Seguridad es nuevamente no imperativa ("teniendo en cuenta la normativa vigente ... por relación al ENS"), no se identifica el órgano responsable de elaborar, aprobar y mantener la política ni se fija su ciclo de revisión periódica. Tampoco se establece la obligatoriedad de un análisis de riesgos formal y documentado como base para determinar las medidas de seguridad, ni se define jurídicamente el Escudo Digital (objeto, gobernanza, ámbito y financiación).

Medidas de adecuación

La ley debería:

- Sustituir la expresión "teniendo en cuenta la normativa vigente en materia de seguridad de las redes y sistemas de información por relación al Esquema Nacional de Seguridad" por "de conformidad con el Esquema Nacional de Seguridad, de aplicación obligatoria en el ámbito de la Administración de la Comunidad de Madrid".

- Atribuir expresamente a la Agencia de Ciberseguridad de la Comunidad de Madrid la elaboración y mantenimiento de la política de seguridad, su elevación al Consejo de Gobierno para aprobación y la supervisión de su cumplimiento en todas las entidades del sector público autonómico.

- Establecer la obligación de revisar la política de seguridad, al menos, **cada dos años** (coincidiendo con el ciclo de auditoría regular del art. 31 del ENS) o cuando se produzcan cambios significativos en el entorno de amenazas, dando cumplimiento al principio de reevaluación periódica del artículo 12 del ENS.

- Dotar de contenido legal al **Escudo Digital**, incluyendo una definición clara, el catálogo de servicios de protección que ofrece, el órgano responsable de su operación (la Agencia de Ciberseguridad), las entidades beneficiarias (sector público autonómico y entidades locales adheridas) y las condiciones de acceso.

3.4.3 Art. 41 — Plataforma de ciberseguridad

Extractos LADIA

- **p. 44 — Art. 41.1**
  - "La Comunidad de Madrid constituirá una Plataforma de ciberseguridad como servicio de prestación centralizado dirigido a proporcionar protección a la Administración de la Comunidad de Madrid y a las entidades locales que a nivel territorial integra."

- **p. 44 — Art. 41.2**

- "Por medio de la Plataforma de Ciberseguridad se aumentará la capacidad de vigilancia y detección de amenazas en la operación diaria de los sistemas de información y comunicaciones, así como mejorar la capacidad de respuesta ante posibles eventuales ciberataques."

- **p. 44 — Art. 41.3**
  - "Los servicios proporcionados por la Plataforma de Ciberseguridad consistirán en:
    a) Prevención de incidentes de ciberseguridad.
    b) Protección de la seguridad.
    c) Detección de incidentes de ciberseguridad.
    d) Gestión, notificación y respuesta ante incidentes de ciberseguridad.
    e) Asesoramiento especializado y apoyo a la gestión de la ciberseguridad.
    f) Recursos y elementos en materia de ciberseguridad.
    g) Formación y concienciación centralizada en materia de ciberseguridad."

Conclusión

El artículo 41 configura la Plataforma de Ciberseguridad como instrumento técnico-operativo central del Título III, con un catálogo de servicios que abarca prevención, protección, detección, gestión de incidentes, asesoramiento, recursos y formación, alineado con las funciones de un CSIRT regional. La inclusión de las entidades locales como beneficiarias es coherente con el mandato de apoyo a las administraciones locales previsto en la Ley 14/2023.

Sin embargo, el precepto adolece de importantes carencias operativas y de gobernanza: no identifica qué organismo será responsable de la operación de la plataforma; no fija niveles de servicio (SLA), tiempos de respuesta garantizados ni criterios de priorización de incidentes; los servicios descritos son excesivamente genéricos (por ejemplo, "protección de la seguridad" carece de contenido técnico definido). Además, no se prevé la obligación de conexión de las entidades al sistema ni un modelo de gobernanza compartida con las entidades locales. Desde la perspectiva del ENS, resulta indispensable que la plataforma incorpore formalmente los requisitos de gestión de incidentes (registro, clasificación, análisis y comunicación) y la coordinación con el CCN-CERT.

Medidas de adecuación

La ley debería:

- Atribuir expresamente a la **Agencia de Ciberseguridad de la Comunidad de Madrid** la operación y gestión de la Plataforma de Ciberseguridad, en coherencia con su función de CSIRT regional.
- Establecer la obligación de todas las entidades del sector público autonómico de conectar sus sistemas de información a la plataforma y de notificar sus incidentes de ciberseguridad a través de ella, salvo causa justificada.
- Concretar el contenido mínimo de cada uno de los servicios, en particular los de detección y respuesta, incluyendo capacidades como análisis de vulnerabilidades, inteligencia de amenazas, operación de un SOC 24x7 y gestión de SIEM/SOAR, o equivalentes.
- Establecer un modelo de adhesión voluntaria para entidades locales, definiendo compromisos mutuos, catálogo de servicios accesibles y condiciones de uso.
- Prever la **publicación anual de un informe de actividad** de la Plataforma, con estadísticas de incidentes gestionados, tiempos de detección y respuesta, entidades beneficiarias y nivel de cumplimiento del ENS.

3.5 Título IV — Capacitación digital

3.5.1 Art. 44 — Formación del empleado público

Extractos LADIA

- **p. 46 — Art. 44.1**
  - *"La Administración de la Comunidad de Madrid impulsará la formación continua del personal a su servicio [...]"*

Conclusión

El artículo 44 establece la formación continua del personal al servicio de la Administración como una obligación activa, pero no menciona de forma expresa la ciberseguridad como materia prioritaria. Esta omisión contrasta con el artículo 40.3, que sí alude a la capacitación en ciberseguridad como medida de desarrollo de la política de seguridad, y con el mandato de la Ley 14/2023, que atribuye a la **Agencia de Ciberseguridad** el Plan de difusión, formación y concienciación en materia de ciberseguridad.

En su configuración actual, el tratamiento de la formación en ciberseguridad del personal empleado público es insuficiente: no se establece la obligatoriedad de la formación en ciberseguridad para todo el personal, ni se distinguen niveles formativos según el rol (alta dirección, personal TIC, personal general), ni se vincula la formación con marcos de referencia como DigComp o e-CF. Tampoco se prevén indicadores para evaluar la efectividad de los programas de formación (porcentaje de personal formado, reducción de incidentes por error humano, resultados de ejercicios de concienciación, etc.).

Medidas de adecuación

La ley debería

- Establecer la **obligación** de que todos los empleados públicos de la Comunidad de Madrid reciban, al menos, una **formación básica anual en ciberseguridad**, distinguiendo niveles: sensibilización general para todo el personal, formación operativa para personal TIC y gestores de sistemas y formación avanzada en gestión de riesgos para la alta dirección y órganos de gobierno.
- Atribuir a **la Agencia de Ciberseguridad de la Comunidad de Madrid** la definición de los itinerarios formativos en ciberseguridad para empleados públicos, en coherencia con el Plan de difusión, formación y concienciación previsto en la Ley 14/2023.
- Vincular estos itinerarios a los **marcos europeos de competencia digital** (DigComp, e-CF) y a las guías CCN-STIC sobre concienciación y formación.
- Prever la publicación anual de **indicadores de cobertura formativa** (porcentaje de personal formado por nivel y consejería, evolución temporal, resultados de ejercicios prácticos) como parte del sistema de indicadores del artículo 11 de la LADIA.

3.6 Disposición Final Primera

3.6.1 Disposición final primera. Modificación de la Ley 14/2023, de 20 de diciembre, por la que se crea la Agencia de Ciberseguridad de la Comunidad de Madrid

Extractos LADIA

- **p. 50 Uno: modificación del Art. 2 (Ámbito de la Agencia de Ciberseguridad)**
  - *"1. La Agencia ejercerá sus funciones y competencias en el ámbito de la Administración General e institucional de la Comunidad de Madrid con exclusión de las empresas públicas autonómicas con forma de sociedad mercantil, salvo en cuanto participación en el Comité de Seguridad de la Información previsto en el artículo 4 de esta ley, en coordinación con la Agencia de Seguridad y Emergencias Madrid 112 para el ámbito de sus competencias y con todas aquellas entidades y organismos de la Administración General e Institucional de la Comunidad de Madrid con competencias en materia de tecnologías de la información y de las comunicaciones. En el ámbito de las empresas, PYMES y ciudadanos de la Comunidad de Madrid, la Agencia ejercerá sus funciones y competencias en la estricta medida en que sea necesario para la relación con la Administración por medios electrónicos."*

- **p. 50 Dos: modificación del Art. 3 (Funciones de la Agencia de Ciberseguridad)**

- *"La Agencia tiene como objeto la definición, planificación y ejecución de los proyectos y servicios relacionados con la ciberseguridad, así como apoyar e impulsar la capacitación en ciberseguridad y el desarrollo digital seguro de la Región [...]: a) La propuesta al Consejo de Gobierno de la política global de seguridad de la información para la Administración General e institucional de la Comunidad de Madrid. [...] c) La definición, diseño, desarrollo, implantación, mantenimiento, gestión y evolución del modelo de ciberseguridad en la Comunidad de Madrid, que implicará la previa autorización de todo nuevo sistema de información para garantizar el cumplimiento de los requisitos necesarios en esta materia. d) La realización de auditorías de los sistemas de información y de las medidas de seguridad implantadas en los mismos. e) El ejercicio de las funciones de alerta temprana y de ayuda en la respuesta ante amenazas, vulnerabilidades, ataques e incidentes de seguridad a través del CSIRT [...] h) La implantación, evolución y supervisión del Escudo Digital como sistema de seguridad para proteger a la región de ataques y amenazas cibernéticas."*

- **p. 53 Cuatro: modificación del Art. 7.2 (Competencias del consejero delegado)**

  - *"a) Formular y elevar al Consejo de Administración el Plan Estratégico de la Agencia. b) Potenciar y apoyar las actividades de prevención, detección y respuesta del CSIRT, así como la coordinación con la red de CSIRT. c) Formular y elevar al Consejo de Administración el Plan de difusión, formación y concienciación en materia de ciberseguridad. d) Autorizar con carácter previo todo nuevo sistema de información para garantizar el cumplimiento de los requisitos necesarios en esta materia. [...] f) Definir la implantación, evolución y supervisión del Escudo Digital [...] g) Elaborar el informe anual de evaluación de la estrategia global de seguridad de la información de la Comunidad de Madrid. h) Elaborar el Libro Blanco de la ciberseguridad [...] i) Proponer líneas de colaboración en el ámbito de la ciberseguridad con los entes locales de Madrid."*

Conclusión

La Disposición Final Primera introduce las modificaciones más relevantes de la LADIA en materia de ciberseguridad, al ampliar y precisar el catálogo de funciones de la **Agencia de Ciberseguridad de la Comunidad de Madrid** y las competencias de su Consejero Delegado. Se refuerza su papel en la definición de la política global de seguridad de la información, la autorización previa de nuevos sistemas de información, la operación del CSIRT, la implantación del Escudo Digital, la formación y concienciación y la elaboración del Libro Blanco de la ciberseguridad. Estas modificaciones son coherentes con el Plan Estratégico de la Agencia de Ciberseguridad 2025–2028 y dotan de base legal a sus principales líneas de actuación.

No obstante, se aprecian oportunidades de mejora: la delimitación del ámbito funcional respecto a empresas, PYMES y ciudadanos ("en la estricta medida en que sea necesario") puede generar incertidumbre sobre el alcance real del apoyo de la Agencia a estos colectivos; la función de autorización previa de todo nuevo sistema de información carece de desarrollo procedimental (plazos, criterios de evaluación, efectos del silencio), lo que puede comprometer su operatividad; y la coordinación con la Agencia de Seguridad y Emergencias Madrid 112 se enuncia en el artículo 2 modificado, pero no se traduce en mecanismos formales de gobernanza conjunta en la LADIA.

Medidas de adecuación

La ley debería:

- Desarrollar reglamentariamente el **procedimiento de autorización previa de sistemas de información** por parte de la Agencia de Ciberseguridad, fijando plazos máximos de resolución, criterios de evaluación basados en el ENS y efectos del silencio, para garantizar seguridad jurídica y operatividad del control.
- Clarificar el **ámbito de actuación** de la Agencia de Ciberseguridad respecto a empresas, PYMES y ciudadanos, sustituyendo la referencia a la "estricta medida en que sea necesario" por una definición positiva de las funciones de apoyo y fomento del ecosistema y de la cultura de ciberseguridad, coherente con la Ley 14/2023.
- Establecer en la propia LADIA los mecanismos formales de coordinación entre la Agencia de Ciberseguridad de la Comunidad de Madrid y la Agencia de Seguridad y Emergencias Madrid 112, incluyendo la composición y funciones del Comité de Seguridad de la Información y su papel en la supervisión del cumplimiento del ENS en el sector público autonómico.