INFORME
CÁMARA DE COMERCIO DE ESPAÑA

Audiencia e información pública: Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad

Febrero de 2025

1 | INTRODUCCIÓN

El Ministerio del Interior ha abierto el proceso de audiencia e información pública previo a la aprobación del Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad.

El Anteproyecto transpone al ordenamiento jurídico español la Directiva 2022/2555 (NIS-2) en vigor desde el 16 de enero de 2023, cuyo objetivo es fortalecer el marco comunitario de ciberseguridad al establecer requisitos claros para la protección de redes y sistemas de información.

La trasposición de la Directiva NIS2 constituye un hito importante en el ámbito de la regulación de la seguridad digital en España con medidas destinadas a garantizar un elevado nivel de ciberseguridad y contribuir a la mejora de la ciberseguridad en toda la Unión Europea. Además, supone una oportunidad para crear un marco con una regulación homogénea en la materia.

2 | VALORACIÓN GLOBAL

La Cámara de Comercio de España valora positivamente avanzar en la regulación sobre la ciberseguridad, mediante la actualización y mejora del marco jurídico en este ámbito, contribuyendo así a la creación de un entorno favorable y seguro para el desarrollo de la actividad empresarial.

El contenido del Anteproyecto de la Ley de Coordinación y Gobernanza de la Ciberseguridad marca un hito en la protección de los sistemas críticos y la infraestructura digital en España. La transposición de la Directiva Europea NIS2 a la legislación española establece un marco robusto para enfrentar los desafíos actuales en ciberseguridad. La creación del Centro Nacional de Ciberseguridad y la figura del responsable de seguridad de la información fortalecen la resiliencia del ecosistema digital español. Estas medidas no solo buscan proteger las infraestructuras esenciales, sino también fomentar una cultura de seguridad que involucre a todos los actores del sector público y privado. En última instancia, la implementación efectiva del contenido de este Anteproyecto de Ley pretende garantizar la seguridad y confianza en el entorno digital, promoviendo así el desarrollo económico y social del país.

Por otra parte, el nuevo marco normativo impone obligaciones estrictas a las entidades esenciales e importantes, que deberán adoptar medidas avanzadas de gestión de riesgos, notificación de incidentes y certificación de seguridad. El régimen sancionador previsto refuerza el cumplimiento, con multas significativas para quienes incumplan sus responsabilidades. Sin duda, estas exigencias suponen un reto para las empresas, además de un coste que debe ser equilibrado y proporcional, al tiempo que representan una oportunidad para consolidar estándares más elevados de ciberseguridad y competitividad en el mercado global.

Por último, y desde la necesaria armonización europea en la materia, el objetivo de un mercado único pasa porque en cada uno de los países integrantes de la UE no se establezcan ámbitos adicionales en los sectores concernidos y por la no introducción de medidas añadidas que restrinjan el comercio en el mercado único de la UE.

3 | OBSERVACIONES ESPECÍFICAS

Sobre la base de lo expuesto, a continuación se presentan una serie de observaciones específicas de la Cámara de Comercio de España en el marco de la audiencia pública referida al Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad:

- Modificaciones orientadas a **reducir o eliminar la inseguridad jurídica** que pudiera derivarse de la redacción actual del proyecto de texto normativo. Con el objetivo de garantizar la seguridad jurídica y evitar interpretaciones ambiguas que puedan generar incertidumbre en su aplicación, resulta imprescindible que el Anteproyecto de Ley precise de manera clara y detallada las obligaciones, los sujetos responsables y los criterios de aplicación de sus disposiciones. La falta de concreción en determinados aspectos, como la definición de los órganos de dirección responsables, puede derivar en cargas administrativas desproporcionadas o en divergencias en su interpretación. Más en detalle:

    - El texto del Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad se refiere en 11 ocasiones a la **trasposición de la Directiva (UE) 2022/2557**, como XXX o XXXXXX. Esa trasposición que tenía los

mismos plazos de trasposición que la presente y que como evidencian esas numerosas referencias en este texto de este Anteproyecto de Ley tiene puntos de influencia en la misma, aún no ha sido elevada a información pública.

Este hecho introduce inseguridad jurídica a las empresas puesto que hay aspectos en el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad que hacen referencia a la futura Ley que transponga la Directiva 2022/2557 y de la que aún no se conoce ningún texto preliminar.

- El **artículo 14** del Anteproyecto atribuye a los órganos de dirección de las entidades esenciales e importantes la responsabilidad de aplicar las medidas de gestión de riesgos de ciberseguridad, supervisar su implementación y, en su caso, asumir las consecuencias de su incumplimiento. No obstante, la norma no define con **precisión qué se entiende por órganos de dirección ni especifica el nivel jerárquico al que se extiende esta responsabilidad**, lo que genera una indeterminación que podría derivar en inseguridad jurídica. La falta de concreción respecto a si la responsabilidad recae en el Consejo de Administración, el Comité Ejecutivo, la Alta Dirección o cargos intermedios, como el responsable de Seguridad de la Información, dificulta la asignación clara de obligaciones y sanciones. De hecho, esta ambigüedad resulta contraria al objetivo de la norma, que busca asignar responsabilidades a quienes tienen la capacidad real de dotar de recursos y establecer prioridades estratégicas en la organización. Para garantizar la eficacia del marco de gobernanza, sería recomendable definir expresamente los niveles de responsabilidad dentro de las entidades afectadas.

- **Artículo 31. Medidas de supervisión y ejecución relativas a entidades esenciales.**

  La actual redacción del artículo 31.6 es: "Las personas físicas representantes de las entidades esenciales, así como la autoridad que tenga la competencia para tomar las decisiones en su nombre o ejercer su control, deberá supervisar el cumplimiento de las disposiciones de

esta norma, asumiendo, en su caso, la responsabilidad por el incumplimiento de este deber".

Se propone la siguiente redacción para este artículo: "Las personas físicas **miembros de los órganos de gobierno con competencias en la implantación de esta norma** representantes de las entidades esenciales, así como la autoridad que tenga la competencia para tomar las decisiones en su nombre o ejercer su control, deberá**n** supervisar el cumplimiento de las disposiciones de esta norma, asumiendo, en su caso, la responsabilidad por el incumplimiento de este deber".

En las entidades esenciales sólo tienen capacidad de toma de decisiones que permitan la correcta implantación de los controles requeridos en esta norma las personas y órganos con capacidad ejecutiva. Tal y como recoge el art. 14.1. de esta norma, se establece: "1. Los órganos de dirección de las entidades esenciales e importantes serán responsables de aplicar las medidas para la gestión de riesgos de ciberseguridad incluidas en esta ley, de supervisar su implantación efectiva y, en su caso, asumirán la responsabilidad por su incumplimiento". En este caso se está limitando a los órganos de dirección de las entidades esenciales y no cualquier otra persona que realice funciones de ciberseguridad en la compañía.

Asimismo, en el art. 35.2 de esta norma específica que "2. Los miembros de los órganos de dirección de las entidades responderán solidariamente de las infracciones que éstas cometan", quedando nuevamente acotado a las personas físicas adscritas a los órganos de dirección de las entidades sociales.

Por todo lo anterior, sería necesario matizar en este artículo 31.6 que las personas físicas representantes de las entidades esenciales se circunscriben a las personas físicas que son miembros de los órganos de gobierno, dando continuidad y concordancia al resto de responsabilidades incluidas en la toma de decisiones para la implantación de la norma.

- El **artículo 2**, en su definición de incidente significativo, establece que este se considerará como tal cuando cause graves perturbaciones operativas o pérdidas económicas para la entidad afectada. Sin embargo, no se precisa un umbral cuantitativo para determinar qué pérdidas económicas deben ser consideradas significativas, lo que podría generar incertidumbre en su aplicación práctica. A diferencia de otras normativas, como la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, que emplea criterios objetivos como porcentajes sobre el volumen de negocio anual para la graduación de sanciones, en el texto del Anteproyecto de Ley no se establece una referencia similar. Sería conveniente clarificar si cualquier pérdida económica, por mínima que sea, se incluye en el concepto de incidente significativo o si, por el contrario, solo se considerarán aquellas que alcancen un determinado umbral de magnitud, ya sea en términos absolutos o relativos al volumen de negocio de la entidad afectada.

- **Garantizar la aplicación equilibrada de las obligaciones establecidas en el Anteproyecto de Ley.** Para ello, se podría incorporar un principio de proporcionalidad similar al recogido en el artículo 4.1 del Reglamento de Resiliencia Operativa Digital (DORA)[1]. Concretamente, en el **artículo 3.2**, donde actualmente se establece la aplicabilidad de la norma a determinadas entidades independientemente de su tamaño, podría incluirse un enunciado que disponga que "Las entidades sujetas a esta Ley aplicarán las normas establecidas en el capítulo ... de conformidad con el principio de proporcionalidad, teniendo en cuenta su tamaño y perfil de riesgo general, así como la naturaleza, escala y complejidad de sus servicios, actividades y operaciones". Esta modificación permitiría adaptar las exigencias normativas a la realidad operativa de cada entidad, evitando cargas desproporcionadas para aquellas cuya actividad o dimensión no justifique requisitos excesivos. Además, alinearía el Anteproyecto con otros marcos regulatorios de referencia, como el mencionado Reglamento

[1] Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 y (UE) 2016/1011.

DORA y el Reglamento General de Protección de Datos, que incorporan este principio para asegurar una aplicación efectiva y equitativa de sus disposiciones.

- En relación con el **artículo 15 sobre las medidas generales para la gestión de riesgos de ciberseguridad**, dado el carácter internacional de muchas de las empresas a las que afecta el presente Anteproyecto de Ley, el marco propuesto debería ser lo suficientemente abierto como para incorporar estándares internacionales o globales, y no limitarse exclusivamente a medidas nacionales o europeas. Este enfoque permitiría evitar la creación de marcos de control dispares en función de la regulación vigente en diferentes territorios, lo cual podría resultar en procesos inoperativos y sujetos a incertidumbre.

  En cuanto a la certificación de conformidad prevista para las entidades esenciales, sería oportuno que dicha certificación se base en estándares internacionales reconocidos, lo que facilitaría el cumplimiento no solo de la legislación española o europea, sino también de otras normativas internacionales, como las SEC Rules o NERC CIP.

- Observaciones al **artículo 16. Responsable de seguridad de la información (RSI)**:

  - Modificar el artículo 16.3, en el sentido de otorgar la responsabilidad al Centro Nacional de Ciberseguridad para articular los criterios y mecanismos de acreditación para los RSIs. Así, se propone que el texto se adapte en la siguiente línea: "De conformidad con lo señalado en el artículo 6, el Centro Nacional de Ciberseguridad articulará los criterios y mecanismos con base a los cuales los Responsables de Seguridad de la Información de las entidades del ámbito de aplicación de la presente Ley podrán obtener la acreditación de idoneidad personal y profesional exigida para el mejor desempeño de sus funciones, contemplando, en su caso, aquellas circunstancias particulares que resulten de aplicación a cada sector, grupo de entidades o entidad de que se trate, determinando igualmente los casos en los que tal acreditación pueda resultar voluntaria para el ejercicio profesional de la función de responsable de seguridad antedicha.

La determinación de sus funciones, así como los criterios de idoneidad (personal y profesional) tanto para la obtención, como para el mantenimiento y la pérdida de su condición para el desempeño de sus funciones será responsabilidad del Centro Nacional de Ciberseguridad".

La determinación de la idoneidad (personal y profesional) de los responsables de seguridad es una cuestión de alto impacto, tanto en el sector público como en el privado, por lo que sería conveniente que los criterios a tal efecto fuesen establecidos y aprobados por el Centro Nacional de Ciberseguridad, función que encajaría perfectamente con las funciones de las letras a), b) y e) que le atribuye el art. 6 del Anteproyecto de Ley. De este modo, debería concertarse una formación y conocimiento especifico en una materia tan compleja.

La propuesta tiene el foco en el personal propio de ciberseguridad de las entidades esenciales e importantes, si bien se debería extender al personal de las empresas que prestan servicios de ciberseguridad.

Una alternativa a lo anterior es la modificación del art. 16.3, limitando los requisitos de acreditación y desvinculando su obtención, mantenimiento y pérdida de la Ley de seguridad privada. Proponiendo en este caso el siguiente texto: "en las entidades esenciales, el responsable de la seguridad de la información, su persona física representante en caso de ser un órgano colegiado y su sustituto; independientemente de los requisitos de capacidad técnica, experiencia y formación, deberán obtener la correspondiente acreditación expedida por el Ministerio del Interior, que se limitará a verificar el cumplimiento de los requisitos de idoneidad del solicitante, en los términos que reglamentariamente se establezcan, incluido el mantenimiento y pérdida de la misma. En el caso de tratarse de entidades esenciales que también tengan la consideración de críticas conforme a la ley XXXXXXX, esta obligación será asimismo extensiva al resto de personal de ciberseguridad".

El texto del Anteproyecto, en su actual redacción requiere una acreditación, aportando como única referencia la legislación de la aplicación de la Ley de seguridad privada, donde se abre un abanico amplio de obligaciones; las cuales van desde la realización del curso de Director de Seguridad como parte de la acreditación a una mera declaración responsable. Ello genera tanto inseguridad en los profesionales que actualmente desempeñan sus funciones, como un innecesario debate entre la asimilación de funciones por parte de personal de seguridad privada o que dirige al mismo, y las que desempeña el personal de ciberseguridad, las cuales están asociadas a conocimientos ingenieros y técnicos.

El texto que se propone habilita al Ministerio del Interior para garantizar cierta homogeneidad en las competencias de los responsables de seguridad de la información en la entidades importantes y esenciales, y de su personal en las críticas, con un texto claro, sin referencias ni compromisos con otras legislaciones ajenas. Con la mención expresa al desarrollo reglamentario de esta Ley, confiere además un grado de libertad al Ministerio para determinar esos requisitos.

- **Artículo 16.3 apartado f,** se propone la sustitución de la expresión "vulnerabilidades detectadas" por "vulnerabilidades aprovechadas activamente", con el fin de garantizar un enfoque coherente con la exposición de motivos del texto informado, así como con la transposición de la Directiva NIS2 y la Directiva relativa a la resiliencia de las entidades críticas. Esta modificación resulta oportuna para asegurar la alineación con el Reglamento (UE) 2024/2847 de Ciberresiliencia (*Cyber Resilience Act* o CRA), de modo que la obligación de notificación de vulnerabilidades establecida sea coherente con los criterios recogidos en su artículo 14.1 y en la definición 42 del artículo 3, limitando dicha obligación a las vulnerabilidades que hayan sido efectivamente aprovechadas de forma activa.

Asimismo, cabe señalar que la Directiva NIS2 no impone un requisito de notificación obligatoria de vulnerabilidades, sino únicamente la comunicación de incidentes significativos (artículo 21.1 del texto del Anteproyecto y artículos 4, 13 y 23 de la Directiva NIS2), previendo, en cambio, la comunicación voluntaria de vulnerabilidades (considerandos 58 y 62 y artículo 12.2 de la Directiva NIS2).

- **Artículo 16.3.** Mayor concreción mediante la ampliación de **funciones del responsable de seguridad de la información** (RSI), para reforzar su papel como garante de la gestión de ciberseguridad en las entidades esenciales e importantes, asegurando su participación activa en la toma de decisiones estratégicas y operativas. Para ello, se propone modificar la redacción actual del artículo 16.3, incorporando las siguientes funciones adicionales:

  k) Participar adecuadamente en todas las cuestiones relacionadas con la ciberseguridad.

  l) Con la debida independencia, reportar a los órganos de dirección, al menos, aquellas cuestiones que, por su importancia, gravedad y/o urgencia requieran ser puestas en conocimiento del órgano de dirección, para que estos puedan tomar decisiones estratégicas y operativas sobre posibles riesgos y vulnerabilidades, y supervisar y controlar eficazmente las estrategias y políticas de seguridad implementadas.

  m) De igual manera, deberá reportar al menos anualmente a los órganos de dirección.

  n) Participar en la formación permanente a los órganos de dirección de la entidad.

  La motivación de esta propuesta radica en que el responsable de la seguridad de la información tiene un papel principal en la gestión e implementación de las políticas de ciberseguridad en las entidades

esenciales e importantes y, por lo tanto, es una figura clave a la hora de garantizar su cumplimiento por los órganos de dirección.

Adicionalmente, en este mismo artículo, la actual redacción le confiere el rol de interlocutor con los Equipos de Ciberseguridad y Gestión de Incidentes (CSIRT) y la autoridad de control (apartados f y g, de este Anteproyecto de Ley). Es por ello que las funciones que se proponen y que normalmente ya viene realizando el RSI, en aquellas entidades que tienen nombrado ese responsable, son garantía del cumplimiento de lo establecido tanto en el artículo 14, para los órganos de dirección como para las medidas generales establecidas en el Artículo 15. Medidas generales para la gestión de riesgos de ciberseguridad.

Así, la propuesta de adición de los apartados "l) - m)" ayudaría eficazmente a que los órganos de dirección puedan tomar decisiones estratégicas y operativas, de manera informada, sobre posibles riesgos y vulnerabilidades, y supervisar y controlar eficazmente las estrategias y políticas de seguridad implementadas.

En relación con la propuesta de la inclusión del apartado "m", el responsable de la seguridad de la información debe asumir la elaboración del Informe anual del estado de la seguridad de la información y garantizar su presentación directa al Comité de Dirección. Este último, como máxima autoridad en esta materia dentro de la organización, debe liderar de manera independiente cualquier acción de reporte sobre la seguridad de la información, asegurando su comunicación directa con la dirección de la empresa. Esta independencia jerárquica es esencial para evitar posibles conflictos de interés con otras áreas, como Tecnología de la Información, y garantizar una supervisión objetiva y efectiva de los riesgos y estrategias de seguridad.

Las funciones propuestas no supondrían una injerencia en la organización de la entidad, más allá de las obligaciones concretas que, de forma directa o indirecta esta Ley ya plantea en su actual redacción, sino al contrario, complementariamente a la organización y estructura que la entidad quiera darse a sí misma, estas funciones propuestas del RSI garantizarían

en toda circunstancia que los órganos de dirección responsables de la aplicación de las medidas para la gestión de los ciberriesgos contaran con la información especializada y genuina para tomar las decisiones más adecuadas conforme al riesgo y a la gestión que de los mismos hagan. Estas decisiones informadas tienen especial relevancia a tenor del artículo 35.2 del presente Anteproyecto en el que se indican que serán responsables solidariamente de las infracciones que las entidades cometan.

Se busca así una garantía de cumplimiento similar a la que, para otro ámbito, tiene la figura del Delegado de Protección de Datos (DPD) que el RGPD[2], incluido en el artículo 36 de dicho RGPD, cuando le asigna ese reporte directo, con independencia de la libertad que las empresas y entidades públicas ostentan para establecer su estructura y organización.

- En el mismo sentido al apartado precedente, el **artículo 16, en su apartado 4.d)**, establece que las entidades esenciales deben garantizar que el responsable de Seguridad de la Información mantenga la debida independencia respecto de los responsables de las redes y los sistemas de información. No obstante, la norma no precisa los criterios organizativos y funcionales que deben regir esta independencia, lo que puede generar ambigüedades en su aplicación. Para garantizar una separación efectiva de funciones y evitar posibles conflictos de interés, sería recomendable que la Ley estableciera con mayor claridad los principios que deben guiar dicha independencia.

  La falta de una definición clara de esta independencia organizativa podría comprometer la eficacia del RSI en el cumplimiento de sus funciones, limitando su capacidad de supervisión y de alerta ante riesgos y vulnerabilidades. Por ello, sería conveniente que la norma precisara los criterios que aseguren una independencia real y efectiva, alineándose con los principios establecidos en regulaciones similares, como el rol del Delegado de Protección de Datos en el RGPD.

[2] Reglamento (UE) 2016/679 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.

- El Anteproyecto de Ley por aprobar debe cumplir con los **principios de buena práctica regulatoria (*Smart regulation***). Para ello es imprescindible atender a la necesidad de una "legislación y unas políticas más simples, concretas y fáciles de cumplir y basadas en datos", y en cuya elaboración y aplicación se introduzca el enfoque "una más, una menos", para reducir el impacto regulatorio sobre la ciudadanía y las empresas, en especial las pequeñas y medianas empresas (pymes).

  De particular relevancia es minimizar la carga administrativa derivada de la aplicación de la nueva normativa sobre el tejido productivo. La correspondiente Memoria del Análisis de Impacto Normativo (MAIN) analiza las cargas administrativas que generará para las empresas el cumplimiento de esta nueva norma. La principal carga administrativa se deriva, según indica la citada MAIN, de la habilitación del responsable de seguridad de la información como personal de seguridad privada.

  Sin embargo, el cumplimiento efectivo de la normativa podría suponer cargas administrativas adicionales a las identificadas en la citada MAIN, en tanto en cuanto las empresas deben implementar nuevas infraestructuras y protocolos de seguridad, proporcionar formación al personal, contratar auditorias de seguridad para certificaciones o responder y mitigar los incidentes. Estas actuaciones no solo generan costes económicos, sino también cargas administrativas adicionales derivadas de los procesos necesarios para su ejecución.

- La **disposición adicional quinta** establece que la Ley entrará en vigor el día siguiente a su publicación en el BOE. No obstante, considerando la relevancia y el impacto de la norma, podría ser más adecuado establecer **un plazo de un mes para su entrada en vigor**, permitiendo así que las empresas dispongan de un periodo adicional para adaptarse a las nuevas exigencias. Además, la propia Memoria del Análisis de Impacto Normativo señala expresamente que la entrada en vigor del anteproyecto se producirá un mes después de su publicación en el BOE, lo que evidencia una posible discrepancia que convendría clarificar.

En conclusión, desde la Cámara de Comercio de España, en el desarrollo de la función consultiva que corresponde a esta Corporación conforme a la Ley 4/2014, de 1 de abril, Básica de las Cámaras Oficiales de Comercio, Industria, Servicios y Navegación, se considera positivo avanzar en un marco jurídico que garantice un elevado nivel de ciberseguridad en España y contribuir a una mayor y coordinada ciberseguridad en toda la Unión Europea. Al tiempo, se aportan determinadas observaciones específicas dirigidas a reforzar el actual texto del Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad.