BORR. INFORME
CÁMARA DE COMERCIO DE ESPAÑA

Consulta pública de Comisión Europea relativa a la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la Agencia de la Unión Europea para la Ciberseguridad (ENISA), el marco europeo de certificación de la ciberseguridad y la seguridad de la cadena de suministro de las TIC, y por el que se deroga el Reglamento (UE) 2019/881 (Reglamento sobre la Ciberseguridad 2)

Mayo de 2026

1 | INTRODUCCIÓN

El presente documento constituye la contribución de la Cámara de Comercio de España al proceso de consulta pública abierto por la Comisión Europea sobre la propuesta de Reglamento COM(2026) 11 final – conocida como Reglamento de Ciberseguridad 2 o *Cybersecurity Act* 2 (CSA2) – presentada por la Comisión Europea el 20 de enero de 2026. Esta iniciativa tiene como objetivo principal derogar y sustituir el Reglamento (UE) 2019/881 (Ley de Ciberseguridad) con el fin de adaptar el marco europeo de ciberseguridad a un entorno de amenazas más complejo, a la creciente dependencia de infraestructuras y servicios digitales y a la necesidad de preservar el buen funcionamiento del mercado interior.

En concreto, son cuatro los problemas principales que la presente propuesta de revisión del Reglamento sobre Ciberseguridad pretende abordar: (i) el desajuste entre el marco europeo de ciberseguridad y las necesidades de las partes interesadas; (ii) la aplicación limitada del Marco Europeo de Certificación de la Ciberseguridad; (iii) la fragmentación del panorama normativo de cumplimiento en ciberseguridad; y, (iv) el aumento de los riesgos para la seguridad de las cadenas de suministro de tecnologías de la información y de las comunicaciones (TIC).

La posición de la Cámara parte de una valoración favorable de la finalidad perseguida, condicionada a que el texto final incorpore salvaguardas claras de proporcionalidad, seguridad jurídica, neutralidad tecnológica, apertura competitiva y viabilidad económica para las empresas.

2 | VALORACIÓN GLOBAL

La Cámara de Comercio de España considera oportuna y necesaria la iniciativa de la Comisión Europea de adaptar el marco europeo de ciberseguridad a la evolución del panorama de amenazas y a los nuevos retos estratégicos y normativos, así como de reforzar la seguridad de la cadena de suministro TIC, en un contexto de creciente complejidad geopolítica e interdependencia tecnológica de los sistemas y cadenas de suministro críticos.

La propuesta puede contribuir positivamente a la autonomía estratégica abierta y a la soberanía tecnológica de la Unión, a la reducción de dependencias críticas y a unas

condiciones de competencia más equilibradas frente a operadores de terceros países que no estén sujetos a exigencias equivalentes.

No obstante, ese objetivo debe compatibilizarse con el respeto a la distribución de competencias entre la Unión y los Estados miembros, especialmente en ámbitos estrechamente vinculados con la seguridad nacional, así como con los principios de proporcionalidad y subsidiariedad. Es fundamental que el marco resultante se base en criterios técnicos objetivos, verificables y no discriminatorios, preserve la neutralidad tecnológica y evite restricciones automáticas o desproporcionadas que puedan generar inseguridad jurídica o impactos económicos significativos sobre el tejido productivo.

Asimismo, debe prestarse especial atención a la proporcionalidad empresarial. El incremento de obligaciones puede resultar disuasorio para pymes tecnológicas, integradores, fabricantes de componentes, proveedores de servicios gestionados o empresas usuarias que operan con márgenes reducidos. Un marco eficaz debe acompañarse de guías prácticas, plantillas, plazos razonables, criterios sectoriales y mecanismos de apoyo.

3 | OBSERVACIONES ESPECÍFICAS

Sobre la base de lo expuesto, se presentan a continuación una serie de matices y recomendaciones específicas en el marco de la consulta pública sobre la propuesta de Reglamento COM(2026) 11 final, orientadas a contribuir a unas condiciones de diseño regulatorio que permitan compatibilizar resiliencia, competitividad y seguridad jurídica:

- La propuesta de Reglamento tiene como objetivo derogar y sustituir el Reglamento (UE) 2019/881 (Ley de Ciberseguridad) con el fin de adaptar el marco europeo de ciberseguridad a la evolución del panorama de amenazas y a los nuevos retos estratégicos y normativos. En concreto, la propuesta persigue reforzar el mandato de ENISA, reformar y ampliar el Marco Europeo de Certificación de la Ciberseguridad, mejorar la coherencia del marco normativo y establecer un marco europeo armonizado de seguridad de la cadena de suministro TIC.

  Se considera fundamental garantizar que la propuesta se articule de forma equilibrada, sobre la base de criterios técnicos objetivos y verificables, delimitando con claridad el alcance de la intervención de la Unión respecto de las competencias de los Estados miembros en materias relacionadas con la seguridad nacional y evitando enfoques que puedan generar inseguridad

jurídica, afectar a la neutralidad tecnológica o introducir distorsiones en el mercado interior.

Resulta asimismo recomendable que los procesos de elaboración y mantenimiento de esquemas incluyan consultas tempranas con la industria, publicación de calendarios, evaluación ex post de costes y beneficios, y revisión periódica para incorporar la evolución tecnológica sin generar obsolescencia regulatoria.

- Se considera oportuna la iniciativa promovida por la Comisión para dotar de una mayor coherencia y armonizar la normativa a escala europea (NIS2, CRA, DORA, Cyber Solidarity Act), para adecuar el marco vigente a los nuevos riesgos digitales, así como para reforzar la resiliencia de las cadenas de suministro y mejorar la posición competitiva de las empresas europeas.

  Es importante que la propuesta observe los principios de proporcionalidad y subsidiariedad, evitando generar inseguridad jurídica o nuevas cargas regulatorias desproporcionadas para el tejido empresarial. Se recomienda incorporar de forma expresa el principio de “una sola vez” en la aportación de evidencias: las empresas no deberían verse obligadas a remitir la misma información técnica, contractual o de gobernanza a distintas autoridades o bajo formatos incompatibles cuando la finalidad de supervisión sea sustancialmente equivalente.

  La armonización de notificaciones, especialmente a través de puntos de entrada nacionales únicos y formularios interoperables, debe traducirse en una reducción efectiva de carga administrativa y no solo en una redistribución formal de canales. Resulta igualmente conveniente alinear definiciones, umbrales, plazos y taxonomías de incidentes con NIS2 y con los futuros mecanismos de notificación centralizada.

  Asimismo, se considera importante que las medidas que se adopten no den lugar a exclusiones generales, obligaciones de sustitución o exigencias adicionales automáticas, sino que respondan a análisis de riesgo transparentes, motivados y revisables, con una mejora de seguridad acreditada y proporcional.

- La propuesta busca reforzar el mandato de la Agencia de la Unión Europea para la Ciberseguridad, avanzar en el desarrollo del Marco Europeo de Certificación de la Ciberseguridad y mejorar la gestión de los riesgos de ciberseguridad de las cadenas de suministro de las TIC.

  Es fundamental que estos objetivos se concreten en un marco basado en criterios técnicos objetivos, verificables y no discriminatorios, que preserve la neutralidad tecnológica, fomente la confianza en el mercado digital europeo y el uso de estándares de seguridad reconocidos globalmente, basados en consenso, y que evite distorsiones que puedan afectar a la competencia, la innovación o la inversión.

- Si bien la propuesta de Reglamento genera una mayor exigencia de gobernanza, independencia y control de riesgos, ofreciendo por ello una mayor claridad jurídica a todos los actores en el mercado de la ciberseguridad, se sugiere valorar enfoques alternativos o complementarios que refuercen la ciberseguridad y, al mismo tiempo, respeten la distribución de competencias y el principio de proporcionalidad.

  En particular, es importante que la gestión de los riesgos vinculados a la seguridad de la cadena de suministro se base en evaluaciones técnicas individualizadas y en medidas de mitigación proporcionadas, que promuevan la resiliencia, la diversificación y unos periodos de adaptación razonables.

  Asimismo, puede valorarse el uso de instrumentos recomendatorios, esquemas escalonados basados en riesgo y mecanismos de reconocimiento de garantías equivalentes, junto con criterios claros, objetivos y no discriminatorios, para mejorar la seguridad sin generar exclusiones generales, cargas financieras desproporcionadas o distorsiones en la competencia, preservando la neutralidad tecnológica, la innovación y la cohesión del mercado interior.

- Se valora positivamente que la propuesta esté orientada a reforzar el papel de la Agencia de la Unión Europea para la Ciberseguridad (ENISA), como punto de central de coherencia y la creación de mecanismos de simplificación y armonización, así como a dotar a ENISA de mayores recursos financieros y humanos para que pueda ejercer eficazmente las nuevas funciones encomendadas.

No obstante, resulta aconsejable que ENISA mantenga un papel estrictamente técnico y que los sistemas de certificación y de notificación se articulen de forma coherente con el resto del marco normativo europeo, evitando duplicidades y cargas innecesarias para los operadores. En particular, la armonización de las obligaciones de notificación a través de puntos de entrada nacionales únicos puede contribuir a mejorar la eficacia del sistema y reducir la complejidad regulatoria.

En todo caso, las orientaciones, especificaciones técnicas y funciones de coordinación de ENISA deben respetar la distribución competencial, proteger información sensible y evitar que criterios de otra naturaleza se presenten como determinaciones técnicas sin motivación suficiente.

- Seguridad jurídica en contratación pública y privada. El Reglamento debería aclarar cómo afectarán los nuevos criterios de riesgo y certificación a contratos ya adjudicados, licitaciones en curso, acuerdos marco, subcontratación y mantenimiento de sistemas existentes. La seguridad jurídica en contratación es esencial para evitar paralización de inversiones, reclamaciones contractuales o divergencias de interpretación entre Estados miembros.

- Proporcionalidad para pymes, mid-caps y empresas usuarias. El tejido productivo español está formado mayoritariamente por pymes, muchas de ellas usuarias intensivas de servicios digitales pero sin equipos especializados de cumplimiento. El Reglamento debe reconocer esta realidad y evitar que la complejidad de los requisitos desincentive la digitalización, la adopción de soluciones europeas o la participación de pymes en licitaciones y cadenas de suministro.

  Se recomienda introducir guías sectoriales, plantillas de cumplimiento, listas de verificación, periodos transitorios diferenciados, herramientas de autodiagnóstico y mecanismos de financiación o bonos de ciberseguridad. Las Cámaras de Comercio pueden desempeñar un papel relevante en la difusión, formación, acompañamiento y canalización de necesidades empresariales hacia las autoridades competentes.

- Evaluación, indicadores y revisión periódica El texto final debería incorporar mecanismos de seguimiento que permitan evaluar si la reforma mejora realmente la seguridad y reduce cargas. Entre los indicadores útiles podrían figurar el tiempo medio de desarrollo de esquemas, número de certificados emitidos y reconocidos, costes de certificación, uso por pymes, reducción de duplicidades de notificación, diversidad de proveedores en sectores críticos y efectos sobre inversión e innovación.

  Se recomienda asimismo prever una cláusula de revisión temprana del funcionamiento del marco de cadena de suministro y de los esquemas de certificación, con participación de las instituciones intermedias de carácter empresarial. Ello permitirá corregir disfunciones antes de que se consoliden cargas innecesarias o divergencias nacionales.

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 estima que la revisión del Reglamento representa una oportunidad estratégica para seguir avanzando en la adaptación del marco europeo de ciberseguridad a la evolución del panorama de amenazas y a los nuevos retos estratégico y normativos, así como para reforzar la seguridad de la cadena de suministro TIC. Al tiempo, se aportan algunos matices y recomendaciones dirigidas a reforzar la propuesta de Reglamento presentada.