Documento de trabajo 6/2021
20 de abril de 2021

Directiva NIS2: valoraciones y posiciones desde el sector privado

Javier Alonso Lecuit

Directiva NIS2: valoraciones y posiciones desde el sector privado

Javier Alonso Lecuit | Investigador sénior asociado, Real Instituto Elcano.

Índice

1. Resumen

La Comisión Europea adelantó a diciembre de 2020 la publicación de la revisión de la Directiva NIS relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad de aquellas entidades que ofrecen servicios esenciales[1].

La propuesta incorpora importantes cambios en relación con las capacidades de supervisión, coordinación y sanción de los Estados miembros, así como novedades dirigidas a aquellas entidades que ofrecen servicios esenciales, con la incorporación de un número significativo de nuevos sectores, incluido el ámbito digital, como los proveedores de servicios en la nube, los servicios y redes de comunicaciones y la Administración Pública. El borrador obliga a las entidades a que adopten un enfoque de la ciberseguridad basado en la gestión de riesgos y amplía los requisitos de ciberseguridad, entre otros, a las relaciones de las entidades con sus cadenas de suministro.

El sector público —y, dentro de él, el Departamento de Seguridad Nacional— lidera la negociación de los cambios al borrador, así como su futura trasposición al ordenamiento nacional. Cuando las empresas que ofrecen servicios esenciales se encuentran en plena fase de implantación de las medidas establecidas por el desarrollo reglamentario de la trasposición de la anterior Directiva NIS, aprobada en enero de 2021, el Real Instituto Elcano ha creído conveniente consultar a los miembros de su Grupo de Trabajo sobre Ciberpolítica para colaborar con el sector público en el seguimiento y tramitación del actual borrador. Este documento de trabajo refleja el resultado de esa colaboración público-privada, presenta las valoraciones y posiciones sobre la propuesta de Directiva NIS2 de los distintos miembros del Grupo de Trabajo y explora las posibilidades de una mayor colaboración público-privada en el ámbito regulatorio.

2. Punto de partida y antecedentes: la Directiva NIS y su trasposición

La propuesta que se valora actualiza la Directiva relativa a la seguridad de las redes y sistemas de información (Directiva NIS), aprobada en 2016, primer acto legislativo a escala de la UE en materia de ciberseguridad, que ha contribuido a armonizar y mejorar las capacidades europeas mínimas de respuesta en materia de ciberseguridad.

A escala nacional, la Directiva NIS ha obligado a los Estados miembros a adoptar estrategias nacionales de ciberseguridad, a designar autoridades de ciberseguridad y a supervisar el cumplimiento de requisitos mínimos en materia de ciberseguridad y de notificación de los incidentes a los operadores designados de servicios esenciales y servicios digitales. También ha facilitado el intercambio de información estratégica y operativa entre los Estados y ha mejorado la ciberresiliencia de las entidades públicas y privadas de siete sectores (energía, transporte, banca, infraestructuras de los mercados financieros, sanidad, suministro y distribución de agua potable, e

[1] Por defecto, salvo que se indique un tipo de entidad en concreto, se entenderán éstas en un sentido amplio, es decir, todas aquellas “entidades” obligadas por la Directiva NIS en los Anexos II (“Tipos de entidades a efectos del artículo 4, punto 4”) y Anexo III (“Tipos de servicios digitales a efectos del artículo 4, punto 5”) o las correspondientes “entidades esenciales” y “entidades importantes” establecidas en los Anexos I y II de la Propuesta NIS2.

infraestructuras digitales) y transversalmente en tres servicios digitales (mercados en línea, motores de búsqueda en línea y servicios de computación en la nube).

La trasposición de la Directiva NIS a través del Real Decreto Ley 12/2018, de 7 de septiembre, ha contribuido a crear una cultura común en torno a la ciberseguridad en las empresas que ofrecen servicios esenciales ante los complejos retos que implica la seguridad de las redes y sistemas de TIC, marcando un hito en la forma en que ha sido abordada por las autoridades públicas de los Estados miembros internamente y a nivel de cooperación europea. El tardío desarrollo reglamentario (Real Decreto 43/2021, de 28 de enero) ha retrasado y dificultado la puesta en práctica de las medidas establecidas en la Directiva NIS y ha generado incertidumbre e inseguridad jurídica entre las empresas de servicios esenciales —coincidentes en esta fase inicial con aquellas que han sido designadas infraestructuras críticas— y proveedores de servicios digitales afectados.

Las Administraciones Públicas son operadores de servicios esenciales y, al mismo tiempo, la autoridad competente para su regulación y desarrollo reglamentario. En particular, deben gestionar los incidentes, potenciar y coordinar la respuesta ante retos para la ciberseguridad como el *ransomware* o el *phishing*, proteger la privacidad y combatir el ciberdelito que amenaza la propia supervivencia de las empresas. Aunque las Administraciones Públicas son el núcleo esencial de la gobernanza de la ciberseguridad en España, la colaboración público-privada va a ser más necesaria en los próximos años, no sólo para asegurar un relevo ordenado entre las directivas NIS y NIS2, sino también para velar por la coherencia entre las anteriores y otras propuestas normativas recientes. Entre otros retos a corto plazo, el sector público tiene que:

- desarrollar y aplicar los potenciales del marco regulador vigente de ciberseguridad (Real Decreto Ley 12/2018 y Real Decreto 43/2021), incluyendo la actividad sancionadora;
- añadir a los esquemas nacionales de certificación la implantación de los esquemas comunes de certificación a nivel europeo derivados del Reglamento sobre la Ciberseguridad de 2019 (Cybersecurity Act);
- ganar protagonismo e influencia en los foros europeos e internacionales donde se está configurando la gobernanza internacional de la ciberseguridad;
- canalizar los significativos recursos del Next Generation Plan para actualizar los niveles de ciberseguridad exigidos en las Administraciones Públicas y la generación y retención de talento en el sector privado y en el resto de la sociedad;
- apoyar a través de la colaboración público-privada la seguridad de las empresas españolas que prestan servicios esenciales e infraestructuras críticas;
- mejorar la bidireccionalidad y transparencia en el intercambio de información e inteligencia con las entidades privadas en las materias en las que sea posible, en particular en lo relativo a la gestión de ciberincidentes.

Junto a estos retos a corto plazo, las Administraciones Públicas tienen que afrontar a medio plazo la implantación y actualización de las medidas relacionas con la seguridad de los sistemas y redes de información (directivas NIS y NIS2). Estos son los ámbitos

regulatorios que se analizan en este documento de trabajo y para el que se proponen numerosos ámbitos de mejora, entre ellos:

- Aumentar la coordinación entre las distintas autoridades competentes, fijar con claridad de cara a ciudadanos y empresas el reparto de competencias entre los distintos actores y aumentar los medios materiales y humanos, dado que la futura Directiva NIS2 exigirá una mayor capacidad de supervisión a las autoridades competentes.
- Promover una mayor cooperación público-privada. Si en algún ámbito es especialmente importante es en la gestión de la ciberseguridad, en la cual gran parte de las capacidades están en el sector privado.
- Extender con claridad el ámbito de aplicación de la Propuesta NIS2 a operadores de servicios esenciales no críticos, con un nivel de obligaciones menor, para lograr un nivel uniforme básico obligatorio. Incluir asimismo ciertas orientaciones y obligaciones básicas de cumplimiento para pequeñas y medianas empresas.
- Introducir en la normativa de contratación pública la obligación de disponer de certificaciones reconocidas en el Esquema Nacional de Seguridad (ENS) para poder licitar contratos públicos. Especificar mayores obligaciones con respecto a los suministradores mediante la inclusión de cláusulas contractuales obligatorias.
- Establecer las auditorías de ciberseguridad como obligatorias y habilitar los perfiles y cualificación de los auditores por parte de la autoridad.
- Introducir obligaciones relativas a la gobernanza interna de la ciberseguridad de las organizaciones y delimitar el rol y obligaciones del responsable de ciberseguridad (CISO), así como la responsabilidad de los consejos de administración.
- Fomentar de forma masiva la cultura de la ciberseguridad en general y especialmente en los niveles educativos obligatorios a través de programas de detección de talento precoz en secundaria.

3. Evaluación de la Directiva NIS

La Comisión adelantó la revisión de la Directiva NIS, prevista para mayo de 2021, dada la necesidad de afrontar nuevos retos como consecuencia de la aceleración del proceso de digitalización, la gravedad y cantidad de ciberincidentes y la creciente interconexión entre los sectores críticos, causas éstas significativamente acentuadas desde el inicio de la crisis del COVID-19. La proliferación de ataques a redes y sistemas de información de alcance transfronterizo, la sofisticación y virulencia de los ataques dirigidos hacia los puntos más vulnerables, tales como los proveedores de la cadena de suministro, y los puestos de teletrabajo de las empresas obligaron a anticipar la revisión y, como resultado, se pudo adelantar la Propuesta NIS2 a diciembre de 2020.

Entre las principales deficiencias encontradas durante el proceso de revisión de la Directiva NIS se pueden señalar las siguientes[2]:

[2] Félix Arteaga, "La evaluación y la revisión de la Directiva NIS: la Directiva NIS 2.0", ARI 19/2021, de 9 de febrero.

- El ámbito de aplicación de la Directiva NIS no encajaba con los sectores transformados por el proceso de digitalización desde su aprobación en 2016 y que ofrecen servicios esenciales para la sociedad, añadido al creciente grado de interconexión entre ellos. Por otra parte, el ámbito de aplicación de los operadores de servicios esenciales no resultaba suficientemente claro en las trasposiciones nacionales, al igual que la competencia de las autoridades nacionales en relación con los proveedores de servicios digitales. Lo anterior no ayudaba a armonizar la designación de operadores de servicios esenciales y, en consecuencia, algunas compañías transnacionales no estaban obligadas a implantar medidas de seguridad o a notificar los incidentes en los Estados miembros en los que operaban.
- La interpretación de la Directiva NIS varió en cada Estado miembro y propició la falta de coherencia entre distintas legislaciones nacionales, con lo que se pudo constatar una gran disparidad en el tipo y número de operadores esenciales designados o en los umbrales de notificación aplicados, entre muchos otros, lo que provocó un desequilibrio en las condiciones de competencia entre las empresas y un alto impacto en su competitividad.
- La Comisión Europea constató un heterogéneo nivel de madurez y capacidad de ciberresiliencia entre las empresas que ofrecen servicios esenciales en la UE, una disparidad de criterios sobre resiliencia aplicados por los Estados y sectores, un escaso nivel de conciencia situacional o, en situaciones de crisis, la incapacidad para ejecutar una respuesta coordinada.
- En la misma línea, la Directiva NIS concedió excesivo margen discrecional a los Estados miembros para establecer los requisitos de seguridad y de notificación de incidentes aplicables a los operadores de servicios esenciales. La falta de armonización en la aplicación de estos requisitos entre distintos Estados dificultó la gestión transfronteriza de incidentes, distorsionó el nivel mínimo europeo de seguridad y creó una carga adicional en aquellas empresas que operan en más de un Estado miembro.
- En contra de lo indicado en la Directiva NIS, los Estados miembros no compartían suficiente información ni de forma sistematizada para generar la necesaria conciencia situacional de la UE, lo que mermaba la eficacia de las medidas de ciberseguridad. Algo parecido ocurría con el insuficiente intercambio de información entre entidades privadas o con el limitado compromiso de colaboración público-privada adquirido a través de los mecanismos de cooperación establecidos a escala de la UE.
- Ya que los Estados miembros han sido reacios a imponer sanciones a las entidades que carecen de las medidas de seguridad apropiadas o que no notificaban incidentes, el régimen de supervisión y ejecución ha resultado ineficaz; este enfoque laxo puede influir negativamente sobre el nivel de resiliencia de determinadas entidades. La dispersión de recursos financieros y humanos destinados por los Estados ha acentuado más si cabe las diferencias en términos de madurez en ciberseguridad y resiliencia entre las compañías de servicios esenciales de los distintos Estados miembros.

Respecto a la experiencia española con la Directiva NIS, no existe una valoración oficial al respecto y tardaría en conocerse, dado el poco tiempo de vigencia de la normativa.

Los *rankings* internacionales, en la medida en que son válidos —la Propuesta NIS2 sí que prevé una valoración del cumplimiento de los Estados miembros—, reflejan el esfuerzo de España para adaptarse al nuevo contexto. Por ejemplo, según el ICT Development Index 2020, de la Unión Internacional de Telecomunicaciones, España ha ocupado el séptimo puesto mundial en compromiso con la ciberseguridad [3]. Aparte de estos, las últimas valoraciones privadas muestran algunas sombras que acompañan a las luces de la trasposición, una valoración que resulta de interés para la negociación de la Propuesta NIS2 y su futura trasposición[4].

4. La intención reguladora de la nueva Directiva NIS2

La propuesta de Directiva NIS2 (Propuesta NIS2), al igual que la Directiva NIS, tiene como objeto establecer un nivel común de ciberseguridad en la Unión armonizando las disposiciones nacionales hacia un nuevo marco regulatorio europeo de ciberseguridad —las directivas, a diferencia de los reglamentos, no pueden transponerse de forma automática, lo que permite un margen de aplicación a los Estados miembros—. Europa se encuentra en una fase de rediseño y armonización del marco integral de ciberseguridad que conjugue los múltiples objetivos en juego: proteger la privacidad y confidencialidad de los datos personales e industriales (RGPD, revisión de la Directiva ePrivacy), establecer mecanismos seguros de identidad digital (Propuesta para una Identidad Digital Europea, revisión del Reglamento eIDAS), garantizar la seguridad de las infraestructuras y servicios de comunicaciones electrónicas (Código Europeo de las Comunicaciones Electrónicas o EECC, 5G Toolbox), lograr la resiliencia de las infraestructuras críticas (Propuesta de directiva relativa a la resiliencia de las entidades críticas) y del sector financiero (Propuesta de reglamento sobre la resiliencia operativa digital del sector financiero o DORA) o definir y aplicar los esquemas europeos de certificación y la ciberdiplomacia europea, entre otros.
En términos generales, la articulación del marco regulatorio se orienta a dar protagonismo a las personas y procesos, no solo a la tecnología. Busca reforzar el marco de gobernanza en las empresas estableciendo responsabilidades para la alta dirección y aporta nuevos incentivos tales como los reputacionales o la seguridad y resiliencia como ventaja competitiva de las entidades reguladas. También ofrece un respaldo a las empresas frente a los grandes suministradores de servicios digitales facilitando la traslación de obligaciones en la relación contractual (por ejemplo, con el reglamento DORA).

En particular, el marco regulatorio aspira a fortalecer la ciberresilencia y la cultura de la ciberseguridad de las entidades que ofrecen servicios esenciales o poseen infraestructuras críticas. En este sentido, existe una fuerte preocupación sobre el grado de madurez de las medianas y grandes empresas no incluidas en los sectores obligados por la regulación en comparación con las que se establecen para los operadores críticos designados, así como por las limitadas capacidades y madurez en el segmento de las

[3] El índice combina once indicadores que parametrizan el grado de madurez alcanzado por los países en relación con la disponibilidad de tecnologías y terminales de acceso a Internet, su utilización y el conocimiento o habilidades respecto a las tecnologías de la información y comunicación.

[4] Vicente Moret, "Dos años de vigencia de la trasposición de la directiva NIS en España: balance de una aplicación heterogénea", ARI 28/2021, de 2 de marzo.

pymes, que forman la mayor parte del tejido industrial nacional. Desde la perspectiva de las organizaciones consultadas, preocupan el número y la consistencia de las normas horizontales y sectoriales por implantar, su impacto en la gobernanza o el coste económico de su implantación y, sobre todo, requieren de las autoridades un marco común que sea sencillo y rápido de implantar.

La Propuesta NIS2 muestra claros avances respecto a la actual Directiva NIS en relación con su ámbito de aplicación y alcance, más claro al dar un segundo nivel de recomendaciones a los agentes no obligados, es decir, incorporar en las políticas de ciberseguridad y gestión de riesgo a grandes empresas y pymes de sectores de actividad no esenciales. La Propuesta NIS2 corrige las deficiencias de la Directiva NIS en lo relativo a la estrategia institucional y transposición de los Estados miembros, entre ellas la ambigua delimitación del ámbito de aplicación de la directiva, lo que se tradujo en diferencias significativas en cuanto a la amplitud y la profundidad de la intervención *de facto* de la UE a escala de los Estados miembros[5]. Como resultado de lo anterior, el nivel mínimo de seguridad de los sistemas de información alcanzado en los Estados miembros no es tan elevado ni tan común como se pretendía. La Propuesta NIS2 mejora también el nivel de armonización de los requisitos de seguridad y notificación para facilitar el cumplimiento de la normativa por parte de las entidades que prestan servicios transfronterizos con el objetivo de mejorar la limitada capacidad de respuesta conjunta que han mostrado hasta la fecha los Estados de la UE en situaciones de crisis.

La ampliación del alcance a nuevos sectores se fundamenta en su criticidad para la economía y la sociedad, en evidencias obtenidas a partir de amenazas reales y en una evaluación de riesgos. Tiene en cuenta la interdependencia de los perfiles de riesgo entre distintos sectores de actividad, las cadenas de suministro y la infraestructura digital compartida por éstos. La práctica coincidencia de los diez sectores esenciales (Anexo I de la propuesta) con los sectores y subsectores identificados en la Propuesta de directiva para la resiliencia de entidades críticas simplifica y da coherencia a ambos marcos regulatorios, orientados a la mejora de la ciberseguridad y la seguridad física. Asimismo, es importante la inclusión de proveedores de comunicaciones electrónicas en el ámbito de las entidades esenciales[6], en particular si se tiene en cuenta la naturaleza transfronteriza de los servicios ofrecidos por proveedores de servicios digitales en Internet —los calificados como NB-ICS y NI-ICS[7], servicios independientes de la red de soporte e incluidos en el ámbito de las comunicaciones electrónicas—.

[5] Por ejemplo, determinados hospitales importantes de un Estado miembro no están incluidos en el ámbito de aplicación de la Directiva NIS, por lo que no están obligados a aplicar sus medidas, mientras que en otro Estado la directiva se aplica prácticamente a todos los proveedores de asistencia sanitaria del país.

[6] Esta mejora está condicionada a que la transposición del Código Europeo de las Comunicaciones Electrónica (EECC) a las regulaciones nacionales de telecomunicaciones evite solapamientos regulatorios en materia de seguridad, lo que provocaría la fragmentación del mercado interno; por ejemplo, en lo relativo a la seguridad 5G.

[7] NB-ICS (*number-based interpersonal communication services*) y NI-ICS (*number-independent interpersonal communication services*): servicios de comunicaciones electrónicas interpersonales independientes de numeración o basados en numeración telefónica, respectivamente.

En consonancia con el mayor alcance de los proveedores de servicios como operadores esenciales, la propuesta establece un régimen de supervisión notoriamente más intrusivo sobre las entidades de servicios esenciales. Las autoridades competentes también tendrán que encargarse de varias tareas nuevas, entre ellas la supervisión de entidades pertenecientes a sectores a los que hasta la fecha no se aplicaba la Directiva NIS. En el mismo sentido, el borrador incorpora auditorías *in situ*, así como otras medidas que llevan parejas severas sanciones por incumplimiento —hasta el 2% de la facturación total—.

Especial relevancia adquiere la armonización y coherencia de la Propuesta NIS2 con otras disposiciones sectoriales y horizontales en materia de ciberseguridad y resiliencia[8]. La Comisión ha de establecer un marco común entre todas ellas que facilite y agilice a las organizaciones su adopción y ofrezca un nivel básico y consistente de ciberseguridad y resiliencia con independencia del sector en cuestión. El legislador debe garantizar la aplicación adecuada y consistente de disposiciones sectoriales para evitar duplicidades o solapamientos. Es igualmente importante cuidar el equilibrio entre la normativa europea y aquella legislación nacional sectorial específica que establezca requisitos adicionales al nivel básico de resiliencia previsto en la Propuesta NIS2 (por ejemplo, el impacto de las futuras leyes nacionales de seguridad 5G), especialmente teniendo en cuenta que se trata de una directiva de armonización de mínimos en un ámbito de competencia exclusiva de los Estados.

Las autoridades regulatorias europeas y nacionales han de garantizar asimismo una aplicación clara del principio *lex specialis* en relación con las propuestas legislativas de carácter horizontal. En particular, la Propuesta NIS2 tendrá que garantizar que no se produzcan solapamientos en las obligaciones o duplicidades respecto a obligaciones de notificación o de aplicación del régimen sancionador establecidas en las distintas propuestas legislativas de ámbito sectorial, orientadas a fortalecer las capacidades y competencias en ciberseguridad y ciberresiliencia prioritarias de cada sector, es decir, reconociendo las diferencias entre sectores.

En cuanto al calendario tentativo previsto para la aprobación y trasposición de la Propuesta NIS2, la propuesta que fue presentada por la Comisión Europea (Dirección DGCOM) al Consejo el 16 de diciembre 2020 se encuentra en fase de análisis y discusión entre los Estados miembros con el propósito de presentar un borrador e informe de progreso en el Consejo Telecom en junio de 2021 y pasar a discusión parlamentaria (Comité de Industria, Investigación y Energía o ITRE) y trílogos para su posterior aprobación en 2022. Entonces los legisladores nacionales tendrían 18 meses para trasponer la nueva directiva.

[8] Entre ellas, la futura legislación relativa a la resiliencia de entidades e infraestructuras críticas, la legislación de protección de datos, la regulación BCE y EBA del sector financiero, la propuesta de reglamento de la UE “Digital Operational Resilience Act” (DORA) o el Código Europeo de las Comunicaciones Electrónicas (EECC),

5. Valoraciones y posiciones preliminares del sector privado

El marco de colaboración público-privada promovido por el Grupo de Trabajo sobre Ciberpolítica del Real Instituto Elcano ofrece la oportunidad de contrastar y trasladar a las autoridades nacionales de ciberseguridad las valoraciones, recomendaciones y propuestas de mejora recogidas dentro del sector privado a propósito del proceso de revisión y aprobación de la Propuesta NIS2. La finalidad de este ejercicio ha sido facilitar al sector público una visión preliminar y desagregada de las distintas posiciones privadas respecto a los artículos más controvertidos.

En términos generales, las entidades consultadas valoran positivamente la iniciativa de la Comisión Europea, aunque son conscientes, tras la experiencia de la directiva vigente, de la dificultad de armonizar la disparidad de normas nacionales en una norma de mínimos y de aplicarla después en la práctica. Entre estas dificultades, cabe citar la adopción de un enfoque de gestión de riesgo en la determinación de los requisitos de seguridad, la adopción de una comunicación coordinada de vulnerabilidades, el intercambio de información entre las autoridades y empresas sobre posibles amenazas o la adopción de una ventanilla única para la supervisión y comunicación de los incidentes, junto con la armonización de los roles y obligaciones legales que deban ejecutar las entidades.

Asimismo, comparten la necesidad de aclarar y mejorar varios puntos del borrador en relación con la armonización entre los distintos marcos regulatorios, cuyas inconsistencias generan importantes ineficiencias e incertidumbre jurídica. Una de las valoraciones más comunes ha sido la dificultad de conciliar las obligaciones establecidas entre distintas regulaciones en lo relativo a la ciberseguridad (RGPD, DORA, EECC, etc.), por ejemplo, a la hora de notificar incidentes. También se ha coincidido en la dificultad de cumplir algunas exigencias de la Propuesta NIS2; por ejemplo, respecto al corto plazo máximo de notificación de incidencias, en relación con los requisitos de notificación de amenazas o sobre las condiciones de uso de cifrado.

5.1 Ámbito de aplicación y alcance de la propuesta

En relación con el ámbito de aplicación y alcance de la propuesta (art. 2), las entidades consultadas del sector privado plantean la necesidad de mejorar los siguientes aspectos de la Propuesta NIS2:

- La consecución de altos estándares de ciberseguridad en la UE precisa asegurar un marco cohesionado y coherente que garantice la seguridad de toda la cadena de valor de extremo a extremo, tal como se analiza más adelante. En este sentido, se considera apropiado haber incorporado al sector público. Sin embargo, resultan insuficientes, principalmente en el sector privado, las medidas de seguridad relativas a la cadena de suministro, en particular vista la contribución al riesgo en relación con las responsabilidades de suministradores de *hardware* y *software* (en adelante HW y SW, respectivamente). El sector público ya obliga a que existan acuerdos de nivel de servicio (*service level agreement* o SLA) y responsabilidades en los pliegos de contratos.
- La incorporación de nuevas entidades calificadas como “importantes” (Anexo II) en el marco de la Propuesta NIS2 debería llevarse a cabo tras una exhaustiva

evaluación del riesgo para evitar que se impongan obligaciones desproporcionadas con respecto al posible riesgo que plantean, con la consiguiente implicación económica en el actual periodo de crisis[9].

- Deben mejorarse la terminología y criterios de diferenciación entre entidades "esenciales" e "importantes", así como las obligaciones que se aplicarían a aquellas entidades que presten varios servicios en la UE y que puedan entrar en el alcance tanto del Anexo I como del Anexo II (por ejemplo, proveedores de servicios digitales). La mejora es importante porque afecta a la seguridad jurídica de las entidades y su inclusión en una categoría u otra debe considerar su ámbito de aplicación y el riesgo intrínseco a cada negocio.
- Aclarar el alcance territorial de la categoría "fabricación" del Anexo II, en particular si se realiza fuera de la UE y si se tiene la intención de incluir en esta regulación procesos de fabricación que excedan el ámbito nacional o europeo.
- Alinear la definición de "servicios de computación en la nube" con la definición establecida en otras regulaciones europeas y estándares.

Un elemento de particular importancia, complejidad y polémica durante las discusiones internas ha sido el debate sobre si ha de incluirse en el ámbito de NIS2 a proveedores de HW y SW. La Propuesta NIS2 no plantea un marco integral sobre la seguridad de los productos y servicios ofrecidos por los suministradores de HW y SW, con lo que el peso de la regulación recae sobre las entidades que proveen servicios esenciales a pesar de destacar la importancia que aquellos adquieren en la seguridad de la cadena de suministro.

La Propuesta NIS2 plantea abordar este reto desde un agregado de soluciones parciales: (1) a través de los contratos cliente-proveedor; (2) con la aplicación de esquemas de certificación, hasta la fecha voluntarios en el sector privado y en fase de definición[10], y (3) mediante la inclusión en el Anexo II ("entidades importantes") de una reducida parte de estos agentes (fabricantes de equipos electrónicos y de ordenadores). Sin embargo, el Anexo II no hace referencia alguna a proveedores de SW, cuando en realidad las amenazas de seguridad más frecuentes y de mayor impacto son causadas por componentes de *software* —considérese además la creciente relevancia del SW en el proceso de virtualización de sistemas IT y en las arquitecturas de comunicaciones electrónicas—.

Algunas opiniones sugieren que los proveedores de HW y SW deben asumir la responsabilidad legal directa sobre los fallos de seguridad desencadenados por sus equipos y servicios y no solo en virtud de la relación contractual, al igual que ocurre en otros sectores, como el de la automoción o el aeronáutico, en los que el fabricante de equipos es responsable de los fallos graves originados por sus componentes. En este sentido, se valora que será necesario profundizar y concretar qué medidas regulatorias mitigarían las amenazas de ciberseguridad originadas por componentes de HW y SW,

[9] El informe de la Comisión sobre la evaluación del impacto de la propuesta calcula que las empresas designadas que se incorporen al marco NIS2 habrán de incrementar un 22% el gasto en TI o un 12% aquellas designadas en la actualidad en el ámbito de aplicación de NIS.

[10] El Esquema Nacional de Seguridad establece las obligaciones que debe exigir la Administración (RD 43/2021, art. 15).

así como los elementos de corresponsabilidad de los agentes que intervienen en el proceso (por ejemplo, debido a la incorrecta configuración del *software* o el parcheo de los *bugs* por parte de quien lo gestione).

Otras valoraciones proponen adoptar un enfoque más ágil y efectivo basado en establecer un ámbito de responsabilidades directas por determinar de los proveedores de HW y SW en el marco de la futura directiva ante el riesgo de que los tres tipos de medidas citados sean un mosaico de soluciones parciales[11]. En esta línea, los proveedores de HW y SW se verían sujetos a requisitos regulatorios mínimos equivalentes a los de los proveedores de servicios esenciales y definidos en una regulación horizontal —tal como se indica en la Estrategia de Ciberseguridad de la UE— con el fin de ofrecer una mejora de la ciberseguridad y de la resiliencia de extremo a extremo de los elementos que intervienen en la entrega de un servicio esencial dado. Restan por concretar los distintos mecanismos que permitan ofrecer estas garantías de mínimos en materia de ciberseguridad y resiliencia.

5.2 Divulgación coordinada de las vulnerabilidades y registro europeo de vulnerabilidades

La industria se cuestiona la conveniencia de establecer un registro de vulnerabilidades centralizado en la UE sin haber establecido previamente un propósito claro. Alternativamente, se propone **analizar la forma de aprovechar las bases de datos existentes para potenciar la coordinación general y limitar la confusión de las entidades recomendando la exclusión de información sobre vulnerabilidades no parcheadas o no mitigadas**. Asimismo, se propone que la Propuesta NIS2 **favorezca un marco de colaboración que permita a los proveedores seguir recibiendo informes directos sobre vulnerabilidades y trabajar en estrecha colaboración con investigadores de seguridad**[12]. Los CSIRT de los Estados miembros deberían ser una opción intermedia para aquellos investigadores de seguridad que prefieran seguir esta vía de colaboración con las entidades.

En todo caso, **ENISA debería publicar información actualizada en línea sobre incidentes de ciberseguridad** que ofrezca un estado de situación general actualizado diariamente y que incluya avisos particularizados por sector en lugar de publicar un informe bienal con información de carácter general. Si las entidades obtuvieran esta información de terceras fuentes, su utilidad podría ser cuestionable debido a inexactitudes e inconsistencias. La industria espera que ENISA informe y coopere con el fabricante del producto o proveedor del servicio de TIC origen de la vulnerabilidad con antelación a la publicación de esta, ya que aquellos han de contar con la oportunidad de enviar a sus clientes actualizaciones o parches que mitiguen los riesgos ocasionados

[11] Por ejemplo, si se trata de un error de día cero (*zero day bug*), el proveedor debería poder corregirlo en un debido tiempo, que se ha de definir dependiendo de la complejidad. Sin embargo, si se trata de un componente de HW o SW fuera de soporte (p. ej. el SO Windows XP), se debería tener en cuenta la responsabilidad del cliente.

[12] En este sentido, sería necesario establecer el marco legal y el impacto que pudiera tener que un proveedor señalara las vulnerabilidades de sus clientes, dado que éstas pueden estar ocasionadas por una configuración incorrecta por parte de sus clientes, un *bug* descubierto que el cliente no ha parcheado, etc.

por la vulnerabilidad antes de que un tercero, en concreto ENISA, lo publique y sea explotado por ciberdelincuentes en detrimento de la ciberresiliencia europea.

5.3 Marcos nacionales de gestión de crisis de ciberseguridad

La colaboración público-privada es imprescindible cuando una entidad se ve afectada por un incidente de ciberseguridad. Abordar la colaboración a través de planes nacionales de respuesta a incidentes ayuda a estar preparados; para ello es fundamental delimitar con claridad los resultados que se espera obtener de la colaboración. En particular, las entidades consultadas señalan la prioridad de mantener el control sobre la gestión de su infraestructura y procesos internos.

En este campo, el sector privado propone **establecer mecanismos en la UE y en los Estados miembros que fomenten y ayuden a tutelar las iniciativas en cooperación**, así como marcos de cooperación e incluso servicios comunes o externalizados a las organizaciones que mejoren tanto las capacidades y especialización requeridas como sus costes, haciéndolos viables y más eficientes sin que por ello las entidades deban delegar a terceros su responsabilidad y control.

Asimismo, el sector privado propone que **las autoridades públicas compartan con las entidades información sobre la gestión de riesgos y la recuperación de incidentes** (art. 7.3.e).

La cooperación entre los CSIRT y las entidades es fundamental; en este sentido, es necesario que el texto aclare aquello que se considera “pertinente” (art. 9.4), así como que concrete —cuantifique— el desarrollo y la priorización de las relaciones con las contrapartes (art. 10.3).

5.4 Implantación efectiva de la cooperación en gestión de crisis

En el ámbito de la cooperación, las entidades consultadas consideran de importancia establecer un marco estándar de ejercicios periódicos de crisis, resiliencia y continuidad de negocio que cuenten con la participación de las cadenas de suministro e involucren a autoridades y reguladores en calidad de observadores con el propósito de lograr una mejora continua en el cumplimiento, cultura, capacitación y entendimiento público-privado. Con este fin, **las entidades esenciales e importantes solicitan participar en la planificación de actividades y ejercicios en el marco de EU-CyCLONe[13] con un interlocutor nacional** (art. 14.2). El refuerzo de la resiliencia implica contar con una visión holística de escenarios, amenazas, vulnerabilidades, riesgos, etc. para construir servicios, infraestructuras y tecnologías guiados por los cinco pilares de la ciberseguridad: (1) prevenir, (2) asegurar, (3) detectar, (4) reaccionar y responder, y (5) recuperar y superar.

Ya que la Propuesta NIS2 establece la posibilidad de participar en el Grupo de Cooperación a agentes privados relevantes (art. 12.3), se considera necesaria **una definición más precisa o ejemplos que aclaren: 1) la participación de la industria**

[13] EU-CyCLONe: European Cyber Crisis Liaison Organisation Network.

y la forma de evaluar esta cooperación (por ejemplo, mediante un programa de trabajo que establezca objetivos claros sobre la cooperación con las entidades); **2) la definición de las entidades privadas "interesadas"**, que permite al sector privado reunirse con el Grupo de Cooperación, discutir sus actividades y compartir futuros desafíos (art. 12.4), y **3) el alcance de "incidente de ciberseguridad a gran escala"** o hacer referencia a las definiciones y taxonomías internacionales ya existentes (art. 14.1).

5.5 Enfoque de gestión de riesgos de ciberseguridad

El enfoque de ciberseguridad incorporado en la Propuesta NIS2, orientado a la gestión de riesgos, representa un avance muy significativo sobre la actual aproximación, basada en el mero cumplimiento normativo. En apoyo de esta línea de trabajo, las entidades privadas consultadas señalan las siguientes consideraciones sobre la Propuesta NIS2:

- Resulta de vital importancia para la industria que la directiva **establezca criterios técnicos, formatos y procedimientos referidos a los estándares, esquemas y protocolos internacionales en la materia**, como por ejemplo la serie ISO 27000, la cual ofrece directrices generales de gestión de riesgos de ciberseguridad junto con una taxonomía, protocolos y formatos asociados de uso común para la descripción de incidentes. Lo anterior no excluye la necesidad de realizar caso por caso una posterior adaptación a las características particulares de cada entidad y sector, identificando aquello que es relevante desde la perspectiva de la gestión de riesgos.
- Igualmente, en relación con el art. 18.2, la redacción final debería incluir **prácticas básicas de higiene informática** tales como la actualización del *software*, la configuración y bastionado de dispositivos, la segmentación de redes, la gestión de identidades y accesos o la concienciación y capacitación del usuario en lo que se refiere a ciberamenazas al correo corporativo (BEC), *phishing* o técnicas de ingeniería social, que son vectores de ataque muy efectivos.
- La obligación de reforzar la seguridad de las comunicaciones mediante **cifrado de extremo a extremo**, señalada en el art. 18.2.g, deja en manos del usuario final el acceso a ellas al impedir la interceptación legal de las comunicaciones por autoridades judiciales y fuerzas de seguridad, lo que aviva el debate sobre la necesidad y riesgos inherentes a las puertas traseras, de gran impacto en la totalidad del ecosistema digital. En consecuencia, los proveedores de servicios digitales solicitan a la Comisión que **reconsidere la necesidad de imponer esta obligación y establezca las contramedidas necesarias en caso de mantenerla.**
- Si bien la industria reconoce la necesidad de identificar, adaptar y gestionar caso por caso las medidas básicas de gestión de riesgos de ciberseguridad para redes y sistemas de información, la Comisión Europea y los Gobiernos habrán de **garantizar que el personal de ciberseguridad no desplace el centro de su actividad al cumplimiento de obligaciones regladas de corte burocrático tales como informar, cumplimentar formularios u otras labores administrativas en detrimento de sus responsabilidades de ciberseguridad**.

- La industria espera de la Comisión Europea, el Parlamento Europeo y los Estados miembros que las medidas de gestión de riesgos de ciberseguridad proporcionen un alto grado de seguridad jurídica a las entidades. Por consiguiente, desde el sector privado consultado se propone modificar el actual borrador para **establecer un conjunto mínimo de estándares internacionales que considerar** (por ejemplo, ISO 27001) **en lugar de hacer referencia al "*estado del arte*"**, término que deja un amplio espacio de interpretación a los evaluadores en el sentido de no haber aplicado todas las capacidades potenciales del "*estado de la arte*" para hacer frente a un determinado incidente.

5.6. Evaluaciones coordinadas de la UE de los riesgos en las cadenas de suministro críticas

La Propuesta NIS2 indica que las entidades son las responsables de aquellas empresas que participen en sus cadenas de suministro y las obliga a tener en cuenta las vulnerabilidades particulares de cada proveedor (art. 18.3). Esta obligación no es realista, dado que numerosas entidades esenciales e importantes tienen una escasa o nula capacidad de control no ya solo sobre las grandes compañías mundiales de IT, sino tampoco sobre compañías con las que habitualmente operan, sea ésta una relación directa o no dependiendo de su posición en la cadena de suministro. Resulta indispensable para el conjunto del sector privado que la Propuesta NIS2 incluya orientaciones con el fin de llevar a la práctica esta obligación. En este sentido, se propone que **aquellas compañías que gestionen un número significativo de clientes estén sujetas a certificaciones basadas en estándares internacionales** —como ISO 27001, citado previamente, u otros (SOC, NIST, C5, ENS, etc.)— **y realizadas por auditores independientes que garanticen que la gestión y mitigación de riesgos se llevan a cabo de forma continua, además de otras iniciativas complementarias y buenas prácticas**[14].

Asimismo, el sector privado propone que la Comisión tenga en consideración iniciativas mundiales lideradas por la industria en esta área, tales como las recomendaciones de la Carta de Confianza para la Ciberseguridad en lo relativo a requisitos de seguridad básicos en la cadena de suministro digital o el fomento de la gestión de riesgos de la cadena de suministro mediante evaluaciones de seguridad externas de los proveedores, productos y servicios (art. 18.2.d). Estos requisitos básicos habrán de complementarse con un enfoque de seguridad por diseño de los productos y servicios.

5.7 Esquemas europeos de certificación de la ciberseguridad

Sobre la utilización de esquemas europeos de certificación, el sector privado consultado incide en tres aspectos. En primer lugar, la propuesta establece que los Estados miembros podrán exigir a las entidades que certifiquen determinados productos, servicios y procesos de TIC en el marco de los esquemas de certificación de

[14] Por ejemplo, la plataforma Pinakes, establecida a partir de la colaboración entre el Centro de Cooperación Interbancaria (CCI) y entidades del sector bancario con certificación LEET Security para la supervisión y homologación, calificación, certificación y auditoría de proveedores de la cadena de suministro, podría ampliarse en un futuro a otros sectores, dado que numerosos proveedores de HW, SW o servicios de TIC o de comunicaciones son comunes a múltiples sectores.

ciberseguridad de la UE para demostrar el cumplimiento de determinados requisitos en relación con las medidas adoptadas para la gestión de riesgos (arts. 18 y 21). Con este propósito, ENISA ha iniciado la definición de los esquemas de certificación sobre criterios de evaluación comunes (*certification common criteria*), sobre servicios en la nube, y sobre componentes 5G.

Sin embargo, esta disposición incide sobre la responsabilidad asignada a las entidades esenciales e importantes en lugar de establecer la obligación para proveedores de HW y SW de certificar aquellos productos, servicios y procesos que ofrecen a las entidades. Por consiguiente, se reitera la **importancia de incluir a los proveedores de HW y SW en el alcance de la futura directiva**, dado que son éstos quienes están mejor emplazados para garantizar la seguridad desde el diseño, siguiendo una aproximación proporcional e implementable definida en función del riesgo, en línea, por ejemplo, con el planteamiento de proveedores de productos y servicios de IT en la Carta de Confianza para la Ciberseguridad.

En segundo lugar, la futura directiva, además de introducir nuevos elementos, debe tener en cuenta la existencia de herramientas nacionales como el Esquema Nacional de Seguridad (ENS) del Real Decreto 3/2010 que ya han demostrado su eficacia a lo largo de los años en el ámbito de la ciberseguridad, evitando solapamientos. Las entidades consultadas consideran el ENS especialmente importante porque desde 2010 se aplica a todo el sector público español —unas 30.000 entidades— y a las empresas que prestan servicios a entidades públicas. Gracias al ENS se dispone de un enfoque común de los principios básicos, requisitos mínimos, medidas de seguridad y procedimientos de auditoría y evaluación de la conformidad mediante la acreditación de las entidades de certificación conforme a la norma ISO/IEC 17065 por parte de la Entidad Nacional de Acreditación (ENAC), así como el seguimiento del estado de las entidades en el ámbito del ENS, lo que justifica sobradamente la necesidad de **aportar por la permanencia del ENS y su coexistencia con los otros esquemas nuevos que puedan implantarse en la UE.**

En tercer lugar, se propone que la futura Directiva NIS2 incluya la **recomendación dirigida a Gobiernos y Administraciones de incluir el requisito de certificaciones de ciberseguridad en los pliegos de los contratos públicos** para incrementar la resiliencia y fomentar una mayor autonomía estratégica europea en la industria e investigación de la ciberseguridad.

5.8 Obligaciones de notificación

La Propuesta NIS2 incorpora obligaciones de información más prescriptivas que la actual directiva. Este enfoque podría ser positivo si condujera a un mayor nivel de armonización entre los Estados miembros. Para ello, es de suma importancia que las obligaciones de información estén claramente definidas, ofrezcan seguridad jurídica a las entidades y autoridades competentes y no impliquen una carga de trabajo desproporcionada para las entidades.

En aras de ofrecer la adecuada seguridad jurídica, las entidades consultadas señalan la necesidad de que la propuesta de directiva y su trasposición definan claramente los

eventos que deban notificarse y el momento de hacerlo. También les preocupa el impacto de las obligaciones sobre las capacidades de gestión de las Administraciones, que pueden verse desbordadas por unas obligaciones de notificación demasiado exigentes. Concretamente, se propone:

- Mejorar la definición sobre qué eventos ("incidentes significativos") deben notificarse, centrándose únicamente en los incidentes relevantes para la provisión de los servicios esenciales, en particular:
  - **Precisar la definición de "ciberamenaza", que es demasiado amplia**[15] (art. 4). Existe el riesgo de que las entidades tengan que notificar cualquier mínima ciberamenaza para asegurar el cumplimiento normativo y evitar sanciones, lo que provocaría la sobrecarga de sus propios mecanismos de denuncia, así como de la capacidad de las autoridades competentes para gestionar dichas notificaciones. La obligación de notificar ciberamenazas que quizás nunca se materialicen desviará la atención y los recursos de las entidades y las autoridades competentes y, lo que es peor, podría ser una fuente de futuros incidentes si esta información llegara a manos de ciberdelincuentes.
  - **Comunicar las ciberamenazas como un aviso en el marco del intercambio voluntario de información, sin obligación reglada de hacerlo ni riesgo de sanción**. La directiva debe incentivar el intercambio informal y voluntario de información sobre ciberamenazas significativas, ya que un elevado número no tienen un impacto real si se han adoptado medidas de seguridad y éstas han sido efectivas.
  - Asimismo, se solicita **una definición más precisa del término "incidente significativo",** ya que el texto actual deja un amplio margen de interpretación. Las empresas exigen mayor seguridad jurídica, en parte debido al severo régimen sancionador. El exceso de incidentes notificados derivado de una interpretación demasiado amplia o conservadora del término puede provocar la devaluación de la información y una saturación de las plataformas de notificación. En la misma línea, es necesario contar con una taxonomía de eventos que facilite un lenguaje común entre los actores, un protocolo de clasificación que ofrezca de forma rápida valoraciones y ponderaciones de impactos y derive a las actuaciones y planes, así como la activación de los comités de crisis.
  - La obligación de notificar "cuasi incidentes" (*near misses*) acrecienta la confusión. Haber reducido el umbral a conatos puede causar una saturación de notificaciones y la disminución de la eficacia de los reguladores. También plantea incertidumbres sobre la procedencia, fiabilidad y atribución de éstas. Por consiguiente, se considera que **la notificación de cuasi incidentes debería ser voluntaria y gestionarse en el marco de los mecanismos de compartición de información** (art.

[15] Hace referencia a la definición establecida en el art. 2.8 del Reglamento de Ciberseguridad (Cybersecurity Act): "cualquier situación potencial, hecho o acción que pueda dañar, perturbar o afectar desfavorablemente de otra manera las redes y los sistemas de información, a los usuarios de tales sistemas y a otras personas".

26) a través de foros como los centros de intercambio y análisis de información (*information sharing and analysis centres* o ISAC).
    - Las entidades recalcan la conveniencia de **intercambiar, dentro de comunidades de confianza establecidas mediante acuerdos marco o convenios, todo tipo de información** que se haya puesto en conocimiento de las autoridades competentes sobre ciberamenazas, vulnerabilidades, indicadores de compromiso, tácticas, técnicas y procedimientos, alertas de ciberseguridad y herramientas de configuración, entre otros. De igual modo, terceras entidades ajenas al alcance de la Propuesta NIS2 podrían enviar notificaciones de forma voluntaria sobre incidentes importantes, conatos o amenazas.
- **Mayor concreción sobre cuándo notificar**. La Propuesta NIS2 establece la obligación de enviar sin dilación la notificación inicial a las autoridades competentes o CSIRT, a más tardar en las 24 horas posteriores al conocimiento del incidente. En una segunda fase, las entidades deberán presentar antes de un mes desde el envío de la notificación inicial un informe final que incluya una descripción detallada del incidente, su gravedad, impacto, causa y las medidas de mitigación adoptadas. A este respecto, desde el sector privado se indica que:
    - El plazo de 24 horas para efectuar la notificación inicial es excesivamente breve y estricto, a pesar de la reducida información que se exige. En el trascurso de las primeras horas del incidente, la prioridad de las entidades es la de mantener sus actividades mientras se resuelva el incidente, por lo que **se debería flexibilizar el plazo**.
    - La notificación **"**desde que se haya tenido constancia del incidente" y con anterioridad a su resolución resulta en ocasiones muy arriesgada, ya que aumenta la vulnerabilidad de las entidades y sus clientes frente a potenciales ataques. Por consiguiente, **la notificación debería ser exigible cuando las entidades tuvieran conocimiento del impacto real del incidente de seguridad y el incidente en cuestión haya afectado significativamente a la prestación del servicio esencial.** Surge la posibilidad de alinear el plazo inicial máximo al del art. 33 del RGPD (72 horas) en aras de una armonización o bien mantener únicamente la referencia a "demoras indebidas", al igual que en la actual Directiva NIS, evitando por defecto establecer un plazo dado de 24 o 72 horas.
    - La obligación de enviar un informe final en el plazo máximo de un mes también es demasiado breve. Un análisis detallado del incidente, su gravedad, causa y las medidas de mitigación tomadas puede llevar mucho más tiempo si lo que se solicita es un informe que contribuya a evitar incidentes similares en el futuro. Es decir, ha de priorizarse por un lado la dedicación de los recursos aplicados a mitigar y resolver el incidente y, por el otro, la calidad del informe frente al plazo de entrega. Por consiguiente, se propone **fijar el plazo máximo transcurridos tres meses desde la notificación inicial del incidente o un mes después de haber finalizado los análisis forenses** —la complejidad de algunos incidentes exige hasta seis meses—. Asimismo, por idénticos motivos,

se propone limitar a las autoridades la solicitud de un solo informe intermedio.

- **Mejorar la definición sobre a quién dirigir las notificaciones** en relación con la referencia a "autoridades competentes o el CSIRT", similar a la de la actual Directiva NIS. A este respecto se proponen los siguientes cambios:
  - Para las entidades y las autoridades competentes es crítico contar con una plataforma única de notificación a nivel nacional y un único punto de contacto, dado el amplio alcance de la directiva, tal como señala el considerando 56 de la propuesta. Es vital asegurar que las entidades concentren sus capacidades en caracterizar y resolver el incidente durante el periodo inicial de resolución, evitando distracciones inducidas por ineficiencias regulatorias. Añadido a lo anterior, existe un alto riesgo de que el solapamiento de notificaciones sobrecargue a las entidades y las autoridades si los procesos de notificación no se simplifican y racionalizan o si no se dota a esas autoridades de los recursos necesarios para gestionarlas. Por consiguiente, solicitan a los Estados miembros que **establezcan un punto de entrada único**, sea el CSIRT de referencia o una de las autoridades competentes, en aplicación del principio *one-stop shopping* ('ventanilla única'), para canalizar la totalidad de las notificaciones requeridas en virtud de la Propuesta NIS2, el RGPD, el Reglamento de privacidad electrónica (ePrivacy), el DORA, la Directiva sobre la resiliencia de las entidades críticas o futuras regulaciones sectoriales en materia de ciberseguridad de ámbito europeo. Este mandato debería trasladarse del considerando 56 al articulado de la propuesta de directiva.
  - En relación con la obligación de notificar a los destinatarios de los servicios "cuando corresponda", **las entidades consultadas solicitan aclaraciones sobre esta condición**, puesto que puede resultar problemática dependiendo de las especificidades de cada incidente de seguridad o acarrear efectos contraproducentes y desconfianza en los clientes, incluso una vez resuelta, y en general en torno al proceso de digitalización.
- Las entidades consultadas consideran que las notificaciones **deberían acompañarse de una función de inteligencia centralizada en un marco de colaboración público-privada** orientada a la mejora de la resiliencia de las entidades y Administraciones y a ofrecer una visión holística sobre ciberincidentes actualizada diariamente, así como avisos diarios específicos por sectores, de modo que las entidades puedan tener conocimiento de los ciberataques denunciados para potenciar las medidas de ciberseguridad.

En la misma línea de potenciar la colaboración público-privada, resultaría de particular relevancia que se incluyera en la futura directiva **un apartado dedicado a la fase de investigación penal de los ciberincidentes**. Habría de fundamentarse en la obligación que adquieren las entidades denunciantes afectadas, su cadena de suministro y sus proveedores de HW y SW de colaborar en tiempo y forma con las fuerzas y cuerpos de seguridad y autoridades judiciales para la identificación de la autoría de los incidentes de naturaleza delictiva. Esta colaboración podría concretarse, por ejemplo, en establecer mecanismos de confianza para el intercambio de inteligencia compartida, así

como en la modulación o incluso anulación de sanciones a aquellas empresas sancionadas que hayan contribuido a la efectiva identificación y captura de los causantes del incidente.

5.9 Consideraciones sobre el alcance y potenciales conflictos en los procesos de notificación

La Propuesta NIS2, al ampliar el alcance y el número de proveedores de servicios catalogados como "entidades esenciales", no tiene en cuenta algunas implicaciones de los esquemas de provisión y operación propios de los servicios en la nube para empresas, en los que un proveedor dado de servicios esenciales es, a su vez, usuario o cliente de un proveedor de servicios esenciales. La propuesta no reconoce las obligaciones contractuales de los proveedores de servicios, lo que podría dar lugar a ambigüedades legales y la superposición en obligaciones de notificación en tanto el proveedor de la nube deba informar a la autoridad sobre un incidente que afecte a su cliente (la empresa de servicios esenciales contratante del servicio digital): tan solo el cliente corporativo puede evaluar el impacto y gravedad del incidente que ha sufrido la entidad esencial que le proporciona la infraestructura o los servicios digitales. Con la Propuesta NIS2 actual, un proveedor de servicios en la nube u otro proveedor de infraestructura digital que se considere esencial se verían obligados a notificar un incidente dado sin contar con información de impacto y de ámbito general de los usuarios finales afectados (los usuarios o clientes finales de la empresa contratante del servicio digital). De la misma manera, la empresa contratante del servicio digital podría ser sancionada por no notificar en tiempo y forma el incidente, aunque el proveedor de servicios digitales se lo hubiera notificado.

Por consiguiente, las entidades privadas proponen **incorporar en la Propuesta NIS2 aclaraciones similares a las de la Directiva NIS, que exige a los operadores notificar cualquier efecto significativo en la continuidad de los servicios esenciales causado por un incidente que afecte al proveedor de servicios digitales** (artículo 16.5)[16], **o unas exenciones de responsabilidad similares** a las de los artículos 14.3 y 16.3 de la directiva[17]. De lo contrario, la notificación (obligatoria) de incidentes sería contraria a las obligaciones de confidencialidad y contractuales del

[16] Directiva (UE) 2016/1148, de 6 de julio, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, art. 16.5: "Cuando un operador de servicios esenciales dependa de un proveedor tercero de servicios digitales para la prestación de un servicio que es esencial para el mantenimiento de actividades sociales y económicas fundamentales, dicho operador notificará cualquier efecto significativo en la continuidad de los servicios esenciales causado por un incidente que afecte al proveedor de servicios digitales".

[17] *Ib.*, art. 14.3: "Los Estados miembros velarán por que los operadores de servicios esenciales notifiquen sin dilación indebida a la autoridad competente o al CSIRT los incidentes que tengan efectos significativos en la continuidad de los servicios esenciales que prestan. Las notificaciones incluirán información que permita a la autoridad competente o al CSIRT determinar cualquier efecto transfronterizo del incidente. La notificación no sujetará al notificante a una mayor responsabilidad"

"Los Estados miembros velarán por que los proveedores de servicios digitales notifiquen sin dilación indebida a la autoridad competente o al CSIRT cualquier incidente que tenga un impacto significativo en la prestación de uno de los servicios a que se refiere el anexo III que ellos ofrezcan en la Unión. Las notificaciones incluirán la información necesaria para que la autoridad competente o el CSIRT puedan determinar la importancia de cualquier impacto transfronterizo. La notificación no sujetará al notificante a una mayor responsabilidad".

acuerdo marco del servicio en la nube. Cualquier desviación equivaldría al incumplimiento del contrato y podría poner en riesgo la reputación del cliente y del proveedor de los servicios digitales.

5.10 Bases de datos de nombres de dominio y datos de registro

El conjunto de los datos de registro de los nombres de dominio incluye tanto datos de carácter personal como no personal (por ejemplo, la información de contacto de la empresa). Gran parte de los datos no son administrados directamente por los registradores de nombres de dominio, sino por los llamados proveedores de servicios de privacidad y *proxy*. A veces, estos proveedores son un servicio que proporciona un registrador, aunque también pueda ofrecerlos un proveedor externo. En cualquier caso, la futura directiva ha de asegurar que el nivel de relación entre un proveedor de servicios de privacidad y *proxy* y un registrador de nombres de dominio dado no dé lugar a ambigüedades con respecto a las responsabilidades en el cumplimiento de las diversas obligaciones establecidas en el artículo 23. Las entidades consultadas consideran que el texto de la Propuesta NIS2 no es suficientemente explícito y proponen que **la definición de "servicios de registro de nombres de dominio"** (artículo 23.1.b) **incluya sin ambigüedades a los proveedores de *proxy* y a revendedores de nombres de dominio** que ofrecen servicios de enmascaramiento de datos y los revendedores que operan en nombre de registradores mayoristas. Por idéntico motivo, se propone **hacer referencia explícita a los proveedores de privacidad y *proxy*** en el artículo 23.5.

Por último, **los datos históricos y un registro permanente de los cambios históricos de los datos son esenciales para la ciberseguridad**. Por ejemplo, los nombres de dominio pueden cambiar de propietario durante un periodo de tiempo y una vez vendidos o transmitidos a otro usuario pueden ser reutilizados con fines ilícitos. En este sentido, es importante **poder identificar al beneficiario final**, es decir, la persona que realmente posee el nombre de dominio, incluso si éste está registrado a otro nombre. Por ello, **el agente mediador debe estar obligado a informar del propietario real del dominio**. Cualquier tipo de anonimato del propietario del nombre de dominio socava efectivamente el valor de seguridad de estos datos.

5.11 Registro europeo de entidades esenciales e importantes

Las entidades reconocen que la mera existencia de un registro que centralice la información de las entidades esenciales e importantes de la UE puede representar en sí misma un riesgo de ciberseguridad. Asimismo, conviene señalar que la UE carece de competencias en materia de seguridad nacional y que tanto la Directiva NIS como la Propuesta NIS2 se enmarcan en las iniciativas de la UE necesarias para establecer el Mercado Digital Único (DSM).
Por consiguiente, se propone que **el registro se implante únicamente a nivel nacional.** La actual propuesta aumentaría la carga administrativa de las entidades esenciales e importantes designadas por las autoridades nacionales.

5.12 Supervisión y ejecución

La Propuesta NIS2 establece un régimen significativamente más estricto e intrusivo que la Directiva NIS o propuestas regulatorias sectoriales *lex specialis* tales como el DORA para servicios financieros. Este cambio de tendencia puede enfriar el clima de estrecha colaboración público-privada en materia de ciberseguridad logrado hasta la fecha entre las entidades del sector privado y las autoridades regulatorias y provocar la merma de confianza del sector privado.

Con el fin de evitar este potencial distanciamiento, las entidades privadas consultadas proponen **acotar con claridad los objetivos y condiciones de aplicación de los mecanismos de supervisión con base en un análisis de proporcionalidad** (inspecciones *in situ*, supervisión a distancia, controles aleatorios, auditorías periódicas, requerimientos de información, etc.) **y asegurar que la ejecución corre a cargo de profesionales debidamente certificados.** Asimismo, será necesario **formalizar canales bidireccionales de comunicación complementarios al régimen de supervisión en el marco de la colaboración público-privada para abordar la resolución de dificultades surgidas en la implantación de la norma**.

A este respecto, **resulta particularmente desafortunada la aproximación basada en en la denuncia pública *(naming and shaming)*** que plantea el borrador (artículo 29.4), ya que desincentiva un cumplimiento regulatorio basado en la excelencia como ventaja competitiva y reputacional y la generación de confianza. Este enfoque puede también tener efectos contraproducentes en las entidades que actúen de buena fe e incentivar atajos y trampas con el propósito de obtener una calificación favorable.

5.13 Régimen sancionador

La Directiva NIS, cuyo régimen sancionador se fundamenta en los principios de efectividad, proporcionalidad y disuasión, ha propiciado trasposiciones a las legislaciones nacionales muy dispares, desde elevadas multas en Reino Unido, España y los Países Bajos a multas máximas más reducidas en Austria, Francia, Alemania e Italia, un resultado distinto al logrado por el RGPD, que es un reglamento de aplicación directa a nivel nacional. Esta experiencia hace que las entidades privadas consideren que, a pesar de mantener idénticos principios rectores, el régimen sancionador apuntado en la Propuesta NIS2 dista de ser proporcionado, especialmente para aquellas entidades que hayan tomado todas las medidas de seguridad que estaban a su alcance y actuado con diligencia. El régimen de supervisión y sancionador ha de ser proporcionado; no debería resultar coercitivo para las entidades para evitar inhibir la aplicación de formas de operar y tecnologías innovadoras en los diferentes sectores. Sin embargo, las sanciones que se proponen en el borrador son excesivas; podrían desincentivar el uso de tecnologías transformadoras como por ejemplo la computación en la nube, que ha demostrado ser particularmente importante para permitir que las organizaciones operen en el entorno del COVID-19.
Las entidades consideran que las multas deberían ser proporcionadas e imponerse únicamente a resultas de un comportamiento negligente (la actual Propuesta NIS2 prevé sanciones máximas a entidades “esenciales” e “importantes” de 10 millones de euros o el 2% del volumen total de negocios). En particular, se propone que **no se impongan sanciones** en virtud del artículo 31 **a menos que la infracción haya sido intencionada**

o de carácter negligente y la entidad hubiera tenido aviso previo sobre la posibilidad de cometer una infracción. Añadido a lo anterior, los proveedores de SW y HW, que desempeñan un importante papel en la seguridad en toda la cadena de suministro, se encuentran exentos de toda responsabilidad reglada en la Propuesta NIS2, ya que estas sanciones se dirigen únicamente a las entidades establecidas en el ámbito de la directiva. Por último, y no menos importante, el sector privado indica que la futura directiva **debería incluir un esquema de sanciones aplicable al sector público en virtud del principio de reciprocidad**, dado que los incumplimientos en materia de ciberseguridad pueden generar riesgos importantes en las entidades privadas.

5.14 Sanciones dirigidas a la alta dirección de las entidades

Las entidades consultadas reconocen la importancia que tiene para su ciberseguridad la exigencia de responsabilidades por la Comisión Europea a los órganos de dirección de las entidades esenciales e importantes, la obligación de implantar en cada entidad una estrategia de ciberseguridad y la necesidad de que los miembros de los órganos de dirección cuenten con especialistas en seguridad de IT adecuadamente cualificados. Sin embargo, las entidades echan en **falta un reconocimiento reglado de la figura del responsable de ciberseguridad de las entidades esenciales e importantes designadas** —la omisión de la figura de los CISO no favorece la necesaria especialización de los responsables—.

Dicho esto, puede resultar cuestionable que los miembros de los órganos de dirección deban recibir formación sobre ciberseguridad a pesar de los beneficios relativos a la concienciación en esta materia o que los informes realizados por el CISO o el responsable de seguridad de IT no proporcionen información comprensible y pormenorizada a los comités de dirección. Asimismo, puede considerarse excesiva la responsabilidad que adquieren los miembros de la alta dirección por el incumplimiento de la Propuesta NIS2, especialmente si el objetivo central es garantizar una adecuada concienciación sobre la ciberseguridad en las empresas.

No obstante, si la Comisión Europea establece de obligado cumplimiento la formación sobre ciberseguridad en los miembros de la alta dirección de las entidades, se propone que **se defina con claridad qué constituyen "conocimientos y destrezas suficientes**" a fin de delimitar qué habilidades se consideran adecuadas para su cumplimiento. Igualmente, se propone que la futura Directiva NIS2 **defina claramente qué roles, funciones y comités son exigibles como mínimo a las entidades —sean públicas o privadas— y su cadena de suministro en el ámbito de la ciberseguridad, junto con la designación de un miembro de la alta dirección como responsable de los riesgos tecnológicos al que sí pueda exigirse la adecuada formación**. Estas recomendaciones habrán de ser consistentes entre todos los Estados miembros con el fin de garantizar que los órganos de dirección no se enfrenten a requisitos divergentes en distintos Estados de la UE.

6. Propuestas para la colaboración público-privada

En este momento de profunda transformación, los Estados están movidos a cambiar sus métodos y formas tradicionales de actuar. Los Estados nacieron hace 500 años como

una estructura para asegurar la vida y los derechos de los ciudadanos, para protegerlos frente a amenazas. Hoy ese rol sigue siendo tan importante como entonces, solo que las formas de la amenaza han cambiado.

La cooperación público-privada es un instrumento esencial en el ámbito de la gestión de la ciberseguridad en un escenario de digitalización donde la mayor parte de las capacidades y responsabilidades residen en el sector privado.

En este sentido, la colaboración público-privada representa una oportunidad obligada para materializar los potenciales del marco regulador vigente de la Directiva NIS en el Real Decreto Ley 12/2018 y el Real Decreto 43/2021 y preparar el terreno hacia las próximas mejoras que apunta NIS2 formalizando áreas de colaboración conjunta tales como:

1. potenciar la bidireccionalidad en las fases de discusión, posicionamiento y propuesta de enmiendas entre el sector privado y las autoridades legislativas de la propuesta de Directiva NIS2 y su trasposición;
2. establecer canales de comunicación complementarios al propio régimen de supervisión para abordar la resolución de dificultades surgidas en la implantación de la norma, en particular la coordinación y análisis conjunto de la función de supervisión de las entidades por las autoridades;
3. establecer canales bidireccionales para el intercambio de análisis de riesgos y divulgación de mejores prácticas transversales y sectoriales, amenazas, datos de incidencias, respuestas y recuperación de incidentes e inteligencia entre las entidades privadas y las autoridades sectoriales de referencia;
4. impulsar recomendaciones para la sistematización de ejercicios, entrenamientos, capacitaciones y simulaciones; potenciar el desarrollo de productos de ciberseguridad tales como simuladores de amenazas persistentes avanzadas (APT) sobre infraestructuras críticas;
5. definir políticas para la realización periódica de ciberejercicios sectoriales de alcance nacional y trasfronterizo (EU-CyCLONe) que incluyan gestión de crisis, resiliencia y continuidad y que involucren a las cadenas de suministros de las empresas participantes;
6. establecer mecanismos de confianza para potenciar las capacidades de inteligencia compartida entre el sector privado, las fuerzas y cuerpos de seguridad y las autoridades judiciales en el marco de la resolución de las investigaciones criminales de los ciberincidentes;
7. establecer políticas que potencien la cultura, formación, capacitación y talento.

El extenso y diverso alcance de temas señalado en estos puntos hace necesario para su puesta en práctica que las instituciones públicas y el sector privado concreten programas de trabajo, objetivos e hitos temporales tangibles que faciliten evaluar el progreso alcanzado en la colaboración público-privada en materia de ciberseguridad.

7. Conclusiones y principales propuestas recogidas

Las propuestas señaladas colectivamente en el Grupo de Trabajo por distintas entidades del sector privado nacional para que el sector público las tenga en cuenta durante la revisión del borrador actual de la propuesta y, en su caso, durante la

trasposición de la futura Directiva NIS2 son un reflejo de la colaboración entre la Comisión y las entidades que se ha mantenido a lo largo del proceso de evaluación y revisión de la Directiva NIS. La Comisión comprende la necesidad de la colaboración público-privada e incentiva esa buena práctica desde el principio del proceso regulatorio de las directivas hasta su revisión.

La conclusión de este ejercicio es la necesidad de profundizar la senda de colaboración actual y ampliarla al capítulo de la regulación. La competencia exclusiva de la Administración en materia regulatoria, al igual que la de la Comisión Europea, es compatible con su interacción con los destinatarios de esta para verificar su utilidad y eficacia. Por eso las entidades consultadas se ofrecen a aprovechar la tramitación de la Directiva NIS2 para configurar un marco permanente de colaboración regulatoria.

CLASIFICACIÓN DE LAS PRINCIPALES PROPUESTAS RECOGIDAS

Propuestas de aclaración	• Definir qué roles, funciones y organización son exigibles como mínimo a las entidades —sean públicas o privadas— y su cadena de suministro. • Precisar la definición de entidades “esenciales” e “importantes”, “ciberamenazas”, “cuasiincidentes” e “incidentes significativos”. • Especificar el modo de participación privada en el Grupo de Cooperación de la UE. • Incorporar aclaraciones similares a las que utiliza la Directiva NIS para definir las obligaciones de operadores y proveedores de servicios digitales. • Acotar con claridad los objetivos y condiciones de aplicación de los mecanismos de supervisión con base en un análisis de proporcionalidad, asegurando que la ejecución corre a cargo de profesionales debidamente certificados. • Incluir a los proveedores de *proxy* y a revendedores de nombres de dominio en la definición de “servicios de registro de nombres de dominio”.
Propuestas para el sector público	• Formalizar canales bidireccionales de comunicación complementarios al régimen de supervisión en el marco de la colaboración público-privada para abordar la resolución de dificultades surgidas en la implantación de la norma. • Que las autoridades públicas compartan con las entidades información sobre la gestión de riesgos y la recuperación de incidentes. • Que las entidades esenciales e importantes participen en la planificación de actividades y ejercicios de gestión de incidentes. • Que las obligaciones formales de notificación y gestión no detraigan excesivos recursos y atención de los responsables de sus obligaciones operativas de ciberseguridad. • Que los pliegos de contratación pública incluyan certificaciones de ciberseguridad. • Que se establezca un único punto de entrada o plataforma para las notificaciones originadas desde distintas regulaciones.

	• Que el registro de entidades esenciales e importantes se implante únicamente a nivel nacional. • Que los recursos con los que cuenta el sector público sean adecuados a las obligaciones de supervisión que establezca la Directiva NIS2.
Propuestas para la Comisión Europea	• Incluir a los fabricantes de *hardware* y *software*. • Sopesar la forma y contenido de la divulgación de vulnerabilidades para evitar daños mayores. • Prevenir las inconsistencias entre la futura Directiva NIS2 y el resto de las normas vigentes. • Que los esquemas europeos de certificación preserven el acervo del Esquema Nacional de Ciberseguridad (ENS). • Incluir la figura del responsable de ciberseguridad (CISO) entre los responsables de la alta administración de las entidades esenciales e importantes designadas. • Encuadrar la notificación de incidentes dentro de un marco de inteligencia compartida que beneficie a entidades y Administraciones. • Referenciar las obligaciones a estándares, esquemas y protocolos internacionales. • Que se establezca un único punto de entrada o plataforma para las notificaciones de las distintas regulaciones de ciberseguridad. • Que las obligaciones formales de notificación y gestión de incidentes de la Directiva NIS2 no se hagan en detrimento de las obligaciones de ciberseguridad de las entidades. • Dedicar atención a la fase de investigación penal de los ciberincidentes para que las entidades tengan respaldo y puedan cooperar con las autoridades policiales y judiciales. • Flexibilización de los objetos, plazos y condiciones de las notificaciones. • Restringir las sanciones a los supuestos en que la infracción haya sido intencionada o negligente y con preaviso de las autoridades de supervisión.