AMETIC

Aportaciones al anteproyecto de Ley sobre la seguridad de las redes y sistemas de información

(Transposición al Ordenamiento jurídico español la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión).

Artículo 2. Ámbito de aplicación.
"2. Estarán sometidos a esta ley: *(...)* *b) los proveedores de servicios digitales que tengan su establecimiento principal en España, así como los que, no estando establecidos en la Unión Europea, designen en España a su representante en la Unión para el cumplimiento de la Directiva (UE) 2016/1148 del Parlamento europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.*
El artículo 18 de la Directiva aclara lo que debe entenderse por prestador de servicios digitales con "establecimiento principal" en un Estado Miembro, y es preciso que el Anteproyecto incorpore dicha interpretación. Por ello, **se sugiere la modificación del artículo 2 como sigue:** *"Se considerará que un proveedor de servicios digitales tiene su establecimiento principal en España cuando tengan su sede social en territorio español"*

Artículo 3. Definiciones.
c) Servicio esencial: servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas, que dependa para su provisión de las redes y sistemas de información.
La definición de **servicio esencial** es mucho más amplia de lo previsto en la Directiva. Tal y como está formulada, sería muy difícil discernir entre un servicio esencial y otro que no lo es. Especialmente cuando el texto de la ley refiere a "...**mantenimiento** de las funciones sociales básicas, la salud, la seguridad, **el bienestar social y económico de los ciudadanos**, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas, que dependa para su provisión de las redes y sistemas de información". En consecuencia, con el objeto de cumplir con lo previsto en la Directiva de forma armonizada en Europa, **sería necesario precisar que los servicios esenciales son aquellos que aparecen listados en el Anexo II, de la Directiva 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016**, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

e) Servicio digital: servicio de la sociedad de la información entendido en el sentido recogido en la letra a) del anexo de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
La definición de **servicio digital** también es más amplia de lo previsto en la Directiva. Concretamente, convendría precisar, como indica el artículo 4.5, que se refiere únicamente a los tipos de servicios que figuran en el anexo III de la Directiva. De este modo, la letra a) del anexo de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico al que se refiere el Anteproyecto de Ley, no limita el concepto de servicio de la sociedad de la información a mercado en línea, motor de búsqueda en línea y servicios de computación en la nube, como indica la Directiva en el anexo III, sino que habla de "*todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario.* *El concepto de servicio de la sociedad de la información comprende también los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios.* *Son servicios de la sociedad de la información, entre otros y siempre que representen una actividad económica, los siguientes:* *1.º La contratación de bienes o servicios por vía electrónica. 2.º La organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales. 3.º La gestión de compras en la red por grupos de personas. 4.º El envío de comunicaciones comerciales. 5.º El suministro de información por vía telemática".* Esto va más allá de las facultades que la Directiva otorga a los Estados Miembros en relación con los Prestadores de Servicios Digitales, rompiendo con la ambiciosa armonización en el ámbito europeo. **Por ello, se propone la modificación de este apartado en el siguiente sentido**: *e) Servicio digital: servicio de la sociedad de la información entendido en el sentido recogida en la letra a) del anexo de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, siempre que sea uno de los tipos que figuran en el anexo III de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.*
g) Riesgo: toda circunstancia o hecho razonablemente identificable que tenga un posible efecto adverso en la seguridad de las redes y sistemas de información. Se puede cuantificar como la probabilidad de materialización de una amenaza que produzca un impacto en términos de operatividad, de integridad física de personas o material o de imagen.
La definición de **riesgo** del Anteproyecto de Ley español también va más allá de la definición prevista en la Directiva (art. 4.9), añadiendo que el riesgo *"se puede cuantificar como la probabilidad de materialización de una amenaza que produzca un impacto en términos de operatividad, de integridad física de personas o material o de imagen".* La redacción usada también induce a excluir otras metodologías de análisis de riesgo de eficacia demostrada y/o aceptadas a nivel internacional como las basadas en escenarios, las basadas en la valoración de las dimensiones CID o ACIDA, u otras que en el futuro pudieran desarrollarse.

En un ámbito como el del análisis de riesgos, donde se investigan continuamente posibles metodologías de mayor efectividad que las actuales, la limitación en las metodologías viables puede lastrar significativamente a los sectores públicos y privados nacionales, al obligarles a seguir metodologías de análisis de riesgo subóptimas.

En este sentido, ni la directiva ni los marcos de referencia más reconocidos y/o extendidos a nivel internacional (ISO 27001, NIST SP800) limitan las metodologías de análisis de riesgos aplicables a una única opción.

Teniendo en cuenta que la Directiva faculta a la Comisión Europea, y al Grupo de Trabajo que bajo su amparo se crea, a dictar recomendaciones y actos de ejecución que probablemente maticen e interpreten muchos de los conceptos recogidos en la Directiva, **se propone la supresión de dicho inciso en aras de cumplir con la necesaria armonización a nivel europeo**, y así permitir que términos tan relevantes y que podrían incidir de manera tan significativa en la implementación de las obligaciones de la Directiva como la definición de riesgo tengan una interpretación común en todos los Estados Miembros.

h) Incidente: suceso inesperado o no deseado con consecuencias en detrimento de la seguridad de las redes y sistemas de información.

La definición de **incidente**. Si bien se aplaude la introducción de la referencia a "inesperado o no deseado" a la definición que la Directiva hace sobre incidente, preocupa que se hable de "consecuencias", sin más matización, dado que cualquier mínimo aspecto puede tener consecuencias también mínimas, lo que no justifica su consideración como incidente.

Por ello, **se propone introducir la previsión de la norma europea, modificando el texto del apartado g) del artículo 3 en el siguiente sentido**:

> *"g) Incidente: suceso inesperado o no deseado **con efectos adversos reales** en la seguridad de las redes y sistemas de información".*

s) Servicio de computación en nube: servicio digital que hace posible el acceso a un conjunto modulable y elástico de recursos de computación que se pueden compartir.

El alcance de la directiva no afecta a todo tipo de servicios en la nube. Existen por lo menos tres modalidades:

1. SaaS o Software como servicio.
2. PaaS o Plataforma como servicio.
3. IaaS o Infraestructura como servicio.

Ya que se ha propuesto en el anteproyecto una definición amplia de Cloud Computing, resulta necesario acotar la modalidad del servicio que es relevante para efectos de la directiva. **Se propone el siguiente texto alternativo:**

*s) Servicio de computación en nube: servicio digital que hace posible el acceso a un conjunto modulable y elástico de recursos de computación que se pueden compartir, **en su modalidad de Infraestructura como Servicio o "IaaS".***

Artículo 7. Comunicación de actividad por los proveedores de servicios digitales
Los proveedores de servicios digitales señalados en el artículo 2 deberán comunicar su actividad a la autoridad competente en el plazo de tres meses desde que la inicien, a los meros efectos de su conocimiento.
La forma, punto de contacto y modelo para la comunicación a la autoridad competente del inicio de actividad resulta impreciso. Se debe evitar incumplimiento por desconocimiento. **Se propone señalar explícitamente que se desarrollará reglamentariamente la forma de esta comunicación.** Por los mismos motivos que la ley establece un punto de contacto único para las administraciones públicas de los Estados Miembros, se debe recomendar la existencia de una figura organizativa (CISO) en los OSE y PSD, cuya misión sea la de coordinar internamente la aplicación efectiva de la ley y todas las disposiciones que de ella se deriven, así como servir de punto de interlocución principal con las Autoridades Competentes. **Por ello, se propone agregar el siguiente texto al artículo:** "A efectos de identificar un interlocutor principal en el organigrama del proveedor de servicios digitales para la comunicación y tratamiento de las obligaciones impuestas por la ley se recomienda la identificación y asignación de la figura organizativa de Responsable de Seguridad Corporativa (CISO)"

Artículo 7. Comunicación de actividad por los proveedores de servicios digitales
Los proveedores de servicios digitales señalados en el artículo 2 deberán comunicar su actividad a la autoridad competente en el plazo de tres meses desde que la inicien, a los meros efectos de su conocimiento.
Artículo 9. Autoridades competentes.
1. Son autoridades competentes en materia de seguridad de las redes y sistemas de información las siguientes: *a) Para los operadores de servicios esenciales:* *1º) En el caso de que éstos sean, además, operadores críticos designados conforme a la Ley 8/2011, de 28 de abril, y su normativa de desarrollo: la Secretaría de Estado de Seguridad, del Ministerio del Interior, a través del Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC).* *2º) En el caso de que no sean operadores críticos: la autoridad sectorial correspondiente por razón de la materia, según se determine reglamentariamente.* *b) Para los proveedores de servicios digitales: la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital, del Ministerio de Energía, Turismo y Agenda Digital.* *c) Para los operadores de servicios esenciales y proveedores de servicios digitales que no siendo operadores críticos se encuentren comprendidos en el ámbito de*

aplicación de la Ley 40/2015, de 1 de octubre, de régimen Jurídico del sector público: el Ministerio de la Presidencia y para las Administraciones Territoriales, a través del Centro Criptológico Nacional. *2. El Consejo de Seguridad Nacional, a través de su comité especializado en materia de ciberseguridad, establecerá los mecanismos necesarios para la coordinación de las actuaciones de las autoridades competentes.*
No se prevé un criterio de resolución de dudas para organizaciones que no sepan cómo identificar cual es autoridad competente. Aunque los criterios del artículo 9 son claros, se apoyan en conceptos que se prestan a la confusión y puede provocar desconocimiento y/o aplicación incorrecta por parte de las organizaciones. Esta aclaración resuelve estas dudas. **Se propone designar a criterio del legislador una autoridad competente de entre las designadas en el artículo 9 a la que deben dirigirse las organizaciones como punto de contacto para esta comunicación y para la designación precisa sobre la autoridad que es competente en su caso particular,** en caso de que la organización tenga dudas en la aplicación de los criterios de Artículo 9.

Artículo 10. g) Funciones de las autoridades competentes. **Artículo 14. Cooperación con otras autoridades con competencias en seguridad de la información, y con las autoridades sectoriales.**
Artículo 10. *g) Cooperar, en el ámbito de aplicación de esta ley, con las autoridades competentes en materia de protección de datos de carácter personal, seguridad pública, seguridad ciudadana y seguridad nacional, así como con las autoridades sectoriales correspondientes conforme a lo establecido en los artículos 14 y 29.* *Artículo 14.* *1. Las autoridades competentes, los CSIRT de referencia y el punto de contacto único consultarán, cuando proceda, con los órganos con competencias en materia de seguridad nacional, seguridad pública, seguridad ciudadana y protección de datos de carácter personal y colaborarán con ellas en el ejercicio de sus respectivas funciones.* *2. Consultarán, asimismo, cuando proceda, con los órganos con competencias por razón de la materia en cada uno de los sectores incluidos en el ámbito de aplicación de esta ley, y colaborarán con ellos en el ejercicio de sus funciones.* *3. Cuando los incidentes notificados presenten caracteres de delito, las autoridades competentes y los CSIRT de referencia darán cuenta de ello, a través de la Oficina de Coordinación Cibernética del Ministerio del Interior, al Ministerio Fiscal a los efectos oportunos, trasladándole, al tiempo, cuanta información posean en relación a ello.*
Entre todas las autoridades con las que se cooperará no figuran explícitamente el resto de autoridades competentes ya señaladas en anteriores artículos. Esta necesidad de cooperación sí que se establece para los CSIRT en el artículo 11.2, y de forma no explícita en el artículo 14.

Las autoridades competentes deben cooperar también entre ellas. Es de esperar y la ausencia de esta obligación no resulta adecuada estéticamente.

Se propone la reescritura del Artículo 10, g) como sigue:

"Cooperar, en el ámbito de aplicación de esta ley, con las autoridades competentes en materia de protección de datos de carácter personal, seguridad pública, seguridad ciudadana y seguridad nacional, así como con las otras autoridades competentes conforme a lo establecido en el artículo 9, y con las autoridades sectoriales correspondientes conforme a lo establecido en los artículos 14 y 29."

Artículo 12.1.c).1. Requisitos y funciones de los CSIRT de referencia

1. *Los CSIRT deberán reunir las siguientes condiciones:*

   a) Garantizarán un elevado nivel de disponibilidad de sus servicios de comunicaciones evitando los fallos ocasionales y contarán con varios medios para que se les pueda contactar y puedan contactar a otros en todo momento. Además, los canales de comunicación estarán claramente especificados y serán bien conocidos de los grupos de usuarios y los socios colaboradores.

   b) Sus instalaciones y las de los sistemas de información de apoyo estarán situados en lugares seguros.

   c)Garantizarán la continuidad de las actividades. Para ello:

      1º) Estarán dotados de un sistema adecuado para gestionar y canalizar las solicitudes con el fin de facilitar los traspasos.
      2º) Contarán con personal suficiente para garantizar su disponibilidad en todo momento.
      3º) Tener acceso a infraestructuras de comunicación cuya continuidad esté asegurada. A tal fin, se dispondrá de sistemas redundantes y espacios de trabajo de reserva.

   d) Podrán participar, cuando lo deseen, en redes de cooperación internacional.

Se usa el concepto "traspaso", que no se ha definido y es impreciso. La redacción usada no permite identificar el requisito legal que se deriva de este punto del artículo.

Se propone la eliminación del concepto "traspaso" usando en su lugar un concepto más claro.

Artículo 15.2. Obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales

2. El desarrollo reglamentario de esta ley preverá las medidas necesarias para el cumplimiento de lo preceptuado en el apartado anterior por parte de los operadores de servicios esenciales. Las autoridades competentes podrán establecer mediante orden ministerial, obligaciones específicas para garantizar la seguridad de las redes y sistemas de información empleados por los operadores de servicios esenciales. Así mismo, podrán

dictar instrucciones técnicas y guías orientativas para detallar el contenido de dichas órdenes. *Al elaborar las disposiciones reglamentarias, instrucciones y guías, se tendrán en cuenta las obligaciones sectoriales, las directrices relevantes que se adopten en el grupo de cooperación y los requisitos en materia de seguridad de la información a las que estuviera sometido el operador en virtud de otras normas, como la Ley 8/2011, de 28 de abril, y el Esquema Nacional de Seguridad, aprobado por el Real Decreto 3/2010, de 8 de enero.*
Entre las fuentes de referencia para el diseño de medidas de seguridad citadas en el segundo párrafo de este artículo 15.2 no se citan estándares internacionales, marcos de referencia, cuerpos de conocimiento y otras fuentes de buenas prácticas ampliamente reconocidas y ya utilizadas y desplegadas en empresas del sector privado. La administración debería tomar en consideración como fuente de información (incluso de manera incluso principal) las buenas prácticas ya desarrolladas internacionalmente, que son exigibles y requeridas para otros ámbitos y que se han demostrado efectivas, en los niveles de exigencia solicitados por el mercado. Sería desastroso para la competitividad internacional del sector privado que alguna autoridad competente (incluso sectorial) decidiera de forma autónoma la aplicación de controles de seguridad no consecuentes con los marcos de referencia habituales en el mercado, o en niveles de exigencia superiores, que obligasen a incurrir en costes elevados para el sector privado. Esta regulación no debería influir negativamente en la competitividad del sector por sobre-regulación o sobre-exigencia … menos aún por una exigencia inconsistente con el mercado. **Se propone cambiar la redacción del punto 15.2 como sigue:** "El desarrollo reglamentario de esta ley preverá las medidas necesarias para el cumplimiento de lo preceptuado en el apartado anterior por parte de los operadores de servicios esenciales. Las autoridades competentes podrán establecer mediante orden ministerial, obligaciones específicas para garantizar la seguridad de las redes y sistemas de información empleados por los operadores de servicios esenciales, ***entre ellas la exigencia de auditorías externas y la redacción de proyectos técnicos***. ~~*Así mismo, podrán dictar instrucciones técnicas y guías orientativas para detallar el contenido de dichas órdenes.*~~ "Al elaborar las disposiciones reglamentarias, instrucciones y guías, se tendrán en cuenta las obligaciones sectoriales, _los estándares internacional y marcos de referencia de controles de seguridad generalmente aceptados,_ las directrices relevantes que se adopten en el grupo de cooperación y los requisitos en materia de seguridad de la información a las que estuviera sometido el operador en virtud de otras normas, como la Ley 8/2011, de 28 de abril, y el Esquema Nacional de Seguridad, aprobado por el Real Decreto 3/2010, de 8 de enero."

Artículo 15.3. Obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales
3. Las autoridades competentes deberán coordinarse entre sí y con los diferentes órganos sectoriales con competencias por razón de la materia en lo relativo al contenido y a la aplicación de las órdenes, instrucciones técnicas y guías orientativas que dicten en sus respectivos ámbitos de competencia con objeto de evitar duplicidades en las obligaciones exigibles y facilitar su cumplimiento a los operadores de servicios esenciales.
En la coordinación entre autoridades sobre guías, instrucciones y similares, sólo se indica la posibilidad de duplicidades. Pero no se contempla la posibilidad de inconsistencia entre estos elementos. Resulta más viable el cumplimiento de dos instrucciones duplicadas que pidan el mismo requisito, que dos instrucciones que pidan requisitos diferentes o directamente contradictorios. **Se propone cambiar la redacción del artículo 15.3. como sigue:** "…ámbitos de competencia con objeto de evitar inconsistencias o duplicidades en las obligaciones exigibles y facilitar su cumplimiento a los operadores de servicios esenciales".

Artículo 18. Obligación de Notificación
1. Los operadores de servicios esenciales y los proveedores de servicios digitales notificarán a la autoridad competente, a través del CSIRT de referencia, los incidentes que puedan tener efectos significativos en dichos servicios. Las notificaciones podrán referirse también a los sucesos o incidencias que puedan afectar las redes y sistemas de información empleados para la prestación de los servicios, pero que aún no hayan tenido un efecto adverso real sobre aquellos.
El artículo 18 exige a los operadores de servicios esenciales y a los proveedores de servicios digitales notificar a la autoridad competente los incidentes que pueden tener efectos significativos en los servicios. No obstante, de conformidad con el artículo 16.4 de la Directiva, dicha notificación sólo debe tener lugar por parte de los proveedores de servicios digitales, cuando el proveedor en cuestión *"tenga acceso a la información necesaria para valorar el impacto de un incidente en función de los parámetros que se indican en el párrafo primero".* Es cierto que el artículo 22 del Anteproyecto de Ley prevé que los proveedores de servicios digitales puedan omitir en las comunicaciones que realicen sobre los incidentes que les afecten la información que no dispongan. Pero este precepto no es suficiente para cumplir con lo que la Directiva establece, dado que lo que la misma prevé no es que se omita cierta información cuando no se tenga, sino que hasta que no se disponga de la información necesaria para hacer la evaluación, no se obligue al proveedor de servicios digitales a notificar el incidente. **Por tanto, se propone la modificación del artículo 18, incluyendo un nuevo apartado con el siguiente texto:** *"En el caso de los proveedores de servicios digitales, la obligación de notificar el incidente únicamente se aplicará cuando tengan acceso a la información necesaria para valorar el impacto del incidente en función de los parámetros que se indican en la presente Ley".*

La inclusión de este párrafo es, además, relevante para garantizar que los proveedores de servicios digitales se enfocan en lo verdaderamente importante, que no es otra cosa que resolver potenciales incidentes. Añadir nuevos deberes formales solo conduce a dispersar la atención y consumir recursos que han de destinarse a cumplir con el objetivo perseguido con la Directiva: lograr un elevado nivel común de seguridad de las redes y sistemas de información dentro de la Unión.

Por otro lado, en línea con los comentarios anteriores en relación a la definición de incidente, se propone la eliminación del último inciso del apartado primero del artículo 18:

"1. Los operadores de servicios esenciales y los proveedores de servicios digitales notificarán a la autoridad competente, a través del CSIRT de referencia, los incidentes que puedan tener efectos significativos en dichos servicios. ~~*Las notificaciones podrán referirse también a los sucesos o incidencias que puedan afectar las redes y sistemas de información empleados para la prestación de los servicios, pero que aún no hayan tenido un efecto adverso real sobre aquellos."*~~

Artículo 20. Factores y criterios para determinar la importancia de los efectos de un incidente.
A los efectos de las notificaciones a las que se refiere el artículo 18.1, primer párrafo, la importancia de un incidente se determinará teniendo en cuenta, como mínimo, los siguientes factores: *a) El número de usuarios afectados por la perturbación del servicio esencial.* *b) La duración del incidente.* *c) La extensión o áreas geográficas afectadas por el incidente.* *d) El grado de perturbación del funcionamiento del servicio.* *e) El alcance del impacto en actividades económicas y sociales cruciales.* *f) Importancia de los sistemas afectados o de la información afectada por el incidente para la prestación del servicio esencial* *g) El daño reputacional.*
La redacción original no se ajusta a lo establecido en los artículos 14.4 y 16.4 de la directiva, los factores y criterios para determinar la importancia de un incidente son diferentes para los proveedores que para los prestadores. La importancia de los sistemas y el daño reputacional agregan elementos al reporte de incidentes que consideramos se exceden del campo de la directiva. Por otro lado, el reporte de incidentes quedará finalmente definido en los actos de implementación. **Se propone la siguiente modificación al texto:** *A los efectos de las notificaciones a las que se refiere el artículo 18.1, primer párrafo, la importancia de un incidente se determinará teniendo en cuenta, como mínimo, los siguientes factores:* *Para los operadores de servicios esenciales:* *a) El número de usuarios afectados por la perturbación del servicio esencial.* *b) La duración del incidente.* *c) La extensión o áreas geográficas afectadas por el incidente.* ~~*d) El grado de perturbación del funcionamiento del servicio.*~~

~~*e) El alcance del impacto en actividades económicas y sociales cruciales.*~~ ~~*f) Importancia de los sistemas afectados o de la información afectada por el incidente para la prestación del servicio esencial*~~ ~~*g) El daño reputacional.*~~ *Para los proveedores de servicios digitales:* *a) El número de usuarios afectados por la perturbación del servicio esencial.* *b) La duración del incidente.* *c) La extensión o áreas geográficas afectadas por el incidente.* *d) El grado de perturbación del funcionamiento del servicio.* *e) El alcance del impacto en actividades económicas y sociales cruciales.* ~~*f) Importancia de los sistemas afectados o de la información afectada por el incidente para la prestación del servicio esencial*~~ ~~*g) El daño reputacional.*~~ En cualquier caso, se debería igualmente clarificar el significado y los parámetros medición del requisito "daño reputacional".

Artículo 21. Notificación inicial, notificaciones intermedias y notificación final. Apartado 1
1. Los operadores de servicios esenciales deberán realizar una primera notificación de los incidentes a los que se refiere el artículo 18.1 sin dilación indebida. *La notificación incluirá, entre otros datos, información que permita determinar cualquier efecto transfronterizo del incidente.*
El artículo 21.1 requiere realizar una primera notificación "sin dilación indebida". Pero no se fija un plazo para notificar, aunque sea máximo. Dado que el Reglamento General de Protección de Datos ha establecido un plazo máximo de 72 horas para la notificación, que ya es conocido por las organizaciones y ha sido ampliamente difundido, se considera muy efectivo utilizar también ese plazo. La Directiva no prohíbe ni fija plazo alguno. Este cambio es consistente con el Artículo 22, puesto que este artículo 22 se refiere a las notificaciones intermedias. **Se propone ampliar la redacción del artículo 21.1 a:** "Los operadores de servicios esenciales deberán realizar una primera notificación de los incidentes a los que se refiere el artículo 18.1 _en un plazo máximo de 72 horas desde que el operador identificase el incidente"
Artículo 21. Notificación inicial, notificaciones intermedias y notificación final. Apartado 4
"4. Lo dispuesto en este artículo se aplicará a las notificaciones de incidentes que padezcan los proveedores de servicios digitales sometidos a esta ley en defecto de lo que establezcan los actos de ejecución previstos en los apartados 8 y 9 del artículo 16 de la Directiva (UE) 2016/1148 del Parlamento europeo y del Consejo, de 6 de julio de 2016".
En primer lugar, el artículo 16.10 de la Directiva establece que los Estados no pueden imponer nuevos requisitos de notificación a los proveedores de servicios digitales. Con este apartado

lo que se está haciendo, precisamente, es imponer requisitos que exceden lo previsto en la Directiva, contraviniendo el texto de la misma.

En segundo lugar, es preciso tener en consideración que la introducción de requisitos formales adicionales sólo conducen a distorsionar el principal objetivo de la Directiva: que las empresas resuelvan lo antes posible los incidentes que se detecten. El hecho de añadir nuevas exigencias puede incluso conducir a un fin no deseado: que las empresas opten por notificar absolutamente todo, para eximirse de responsabilidad, saturando los servicios de las administraciones públicas y obviando o dejando para un momento posterior su obligación de reparar el problema detectado.

En consecuencia, se propone la supresión del apartado 4, del artículo 21.

Artículo 23. Incidentes que afecten a servicios digitales
Los operadores de servicios esenciales y los proveedores de servicios digitales sometidos a esta ley, así como cualquier otra parte interesada, que tengan noticia de incidentes que afecten de modo significativo a servicios digitales ofrecidos en España por proveedores establecidos en otros Estados miembros de la Unión Europea, podrán notificarlo a la autoridad competente aportando la información pertinente, al objeto de facilitar la cooperación con el Estado miembro en el que está establecido el citado proveedor. *Del mismo modo, si tienen noticia de que dichos proveedores han incumplido los requisitos de seguridad o notificación de incidentes ocurridos en España que les son aplicables, podrán notificarlo a la autoridad competente aportando la información pertinente.*

El artículo 23 del Anteproyecto introduce un régimen que puede afectar de manera adversa a la armonización y seguridad jurídica pretendida por la Directiva.

En concreto, el artículo 23 del Anteproyecto prevé la posibilidad de que "los operadores de servicios esenciales y los proveedores de servicios digitales sometidos" a la ley española o "cualquier otra parte interesada" notifiquen un incidente de proveedores establecidos en otros Estados Miembros, mientras que la Directiva prevé la obligación de que los propios sujetos obligados sean los que realicen la notificación. El procedimiento previsto por la Directiva es el único que puede otorgar la seguridad jurídica necesaria, ya que sólo los sujetos obligados son capaces de determinar si un determinado suceso constituye un incidente notificable.

Permitir que cualquier otra parte notifique el incidente sólo conllevaría inseguridad jurídica y el bloqueo del sistema. En primer lugar, no se entiende cómo cualquier persona distinta del propio sujeto obligado puede disponer de la información suficiente como para poder tener certeza de que efectivamente se ha producido un incidente notificable. En segundo lugar, y como consecuencia de lo anterior, es preciso tener en cuenta que la incorporación de este cambio respecto al régimen previsto por la Directiva podría implicar un colapso significativo en la labor de las autoridades, que pasarían a recibir un número muy superior de notificaciones al que recibirán otros Estados Miembros también sujetos a la Directiva y que no tengan una regulación al margen de la misma.

De otro lado, este sistema implicaría un alto riesgo de proliferación de notificaciones infundadas y que sólo tendrían como objetivo atacar a los proveedores establecidos en otros

Estados Miembros. Ello implicaría que las autoridades y los prestadores de servicios estén más ocupados intentando gestionar el abundante número de notificaciones recibidas e identificando aquellas que realmente son verídicas y fundadas que promoviendo la correcta aplicación del sistema y trabajando en la mejora de la seguridad.

Todo ello va en contra de los propios objetivos de la Directiva y conduciría al fracaso del sistema.

En consecuencia, se propone la eliminación del artículo 23.

Artículo 25. Información al público.
1. La autoridad competente podrá exigir a los operadores de servicios esenciales o los proveedores de servicios digitales que informen al público sobre los incidentes cuando su conocimiento sea necesario para evitar nuevos incidentes o gestionar uno que ya se haya producido, o cuando la divulgación de un incidente redunde en interés público. *2. La autoridad competente también podrá decidir informar de modo directo al público sobre el incidente.* *En estos casos la autoridad competente consultará y se coordinará con el operador de servicios esenciales o el proveedor de servicios digitales antes de informar al público.*
La decisión sobre comunicación se toma de forma unilateral por el regulador, incluso si la investigación del mismo está en marcha, o incluso si el incidente se ha reportado sin toda la información (artículo 22), o incluso si la difusión del mismo podría advertir al/ a los atacante/s de que su ataque ha sido detectado (mediante uso de honeypots u otras técnicas equivalentes) El loable ánimo de información al público sobre incidentes no debería ser una dificultad ni para la correcta investigación del mismo, ni causar un daño reputacional innecesario a las organizaciones. En ocasiones, la autoridad competente puede no tener una visión completa de los impactos de la comunicación de incidente en la organización que lo está sufriendo, o de la posible pérdida de credibilidad de la autoridad o de la entidad en caso de plantearse dudas o consultas para las que aún no se dispone de respuesta. **Se propone modificar el epígrafe 25.2. como sigue:** “La autoridad competente también podrá decidir informar de modo directo al público sobre el incidente. En estos casos la autoridad competente consultará y se coordinará con el operador de servicios esenciales o el proveedor de servicios digitales antes de informar al público. La autoridad competente no comunicará el incidente cuando la información sobre el incidente sea insuficiente para ofrecer explicaciones adicionales y suficientes a los destinatarios de la comunicación del incidente si fueren pedidas, o si, tras consultar con las autoridades señaladas en los artículos 14.3 o 18.5, se indicase que la difusión del incidente entorpecerá la persecución del posible delito”

Artículo 27. Información anual al punto de contacto único y al grupo de cooperación.
1. Las autoridades competentes transmitirán al punto de contacto único un informe anual sobre el número y tipo de incidentes comunicados, sus efectos en los servicios prestados o en otros servicios y su carácter nacional o transfronterizo dentro de la Unión Europea. *Las autoridades competentes elaborarán el informe siguiendo las instrucciones que dicte el punto de contacto único teniendo en cuenta las indicaciones del grupo de cooperación respecto al formato y contenido de la información a transmitir.* *2. El punto de contacto único remitirá al grupo de cooperación antes del 9 de agosto de cada año, un informe anual resumido sobre las notificaciones recibidas.*
La ley no contiene ninguna previsión relativa al tratamiento histórico de la información sobre incidentes comunicada a las autoridades competentes o a los CSIRT. Una vez comunicado el incidente, resuelto el mismo, y obtenido la información y el aprendizaje posible de un incidente, la utilidad de la información del incidente se limita al análisis estadístico y de tendencias que cabe esperar del informe anual. Una vez agotada esa información, la disponibilidad de esa información en manos de la administración supone un costo de mantenimiento en términos de recursos de almacenamiento, de medidas de protección y en el peor de los casos un riesgo de filtración con consecuencias reputacionales para las entidades que reportaron el incidente. Por eso, parece razonable limitar estos riesgos mediante la eliminación de la información no necesaria. **Se propone agregar en artículo 27.2 lo siguiente:** “El punto de contacto único comunicará a las autoridades competentes y a los CSIRT nacionales la remisión del informe anual, una vez lo haga efectuado.” **Igualmente, se propone la creación de un nuevo Artículo 27.bis. *Periodo de retención de la información sobre incidentes*, con el siguiente texto:** “A la confirmación de remisión del informe anual, las autoridades competentes y los CSIRT eliminarán los datos facilitados por los operadores de servicios esenciales y los proveedores de servicios digitales durante el reporte de incidentes, para todos los incidentes desde cuya fecha de cierre hayan transcurrido más de doce meses, pudiendo conservar únicamente aquellos incidentes que aún no se hayan cerrado, o aquellos que se hayan cerrado en los últimos doce meses. Cada autoridad competente y cada CSIRT mantendrá un registro de los incidentes que se han eliminado en este proceso”

Artículo 30. Autorización para la cesión de datos personales.
Si la notificación de incidentes o su gestión, análisis o resolución requiriera comunicar datos personales, su tratamiento se restringirá a los que sean estrictamente adecuados, pertinentes y limitados a lo necesario en relación con la finalidad, de las indicadas, que se persiga en cada caso. Su cesión para estos fines se entenderá autorizada en los siguientes casos: *a) De los operadores de servicios esenciales y los proveedores de servicios digitales a las autoridades competentes, a través de los CSIRT de referencia.* *b) Entre los CSIRT de referencia y las autoridades competentes, y viceversa.*

c) Entre los CSIRT de referencia, y entre éstos y los CSIRT designados en otros Estados miembros de la Unión Europea. *d) Entre los CSIRT de referencia y otros CSIRT nacionales o internacionales.* *e) Entre el punto de contacto único y los puntos de contacto únicos de otros Estados miembros de la Unión Europea.* *Los datos personales intercambiados se cancelarán cuando dejen de ser necesarios para la finalidad que motivó su cesión y, en todo caso, tras la notificación de cierre del incidente. Con posterioridad, los datos personales serán anonimizados.*
Es necesario introducir otros supuestos para el tratamiento legítimo de datos personales en materia de ciberseguridad para estar en condiciones de asegurar la prevención, protección y resiliencia de las infraestructuras. Por ello se propone el ajustar el redactado e introducir un caso adicional b) al listado "*Si la notificación de incidentes o su gestión,* ***detección,*** *análisis,* ***protección,*** *o resolución requiriera comunicar datos personales, su tratamiento se restringirá a los que sean estrictamente adecuados, pertinentes y limitados a lo necesario en relación con la finalidad, de las indicadas, que se persiga en cada caso. Su cesión para estos fines se entenderá autorizada en los siguientes casos:* **Se propone introducir un caso adicional b) al listado:** a) De los operadores de servicios esenciales y los proveedores de servicios digitales a las autoridades competentes, a través de los CSIRT de referencia. *b) Entre los operadores de servicios esenciales y los proveedores de servicios digitales por lo que se refiere a las incidencias detectadas en la prestación de servicios que se presten.* c) Entre los CSIRT de referencia y las autoridades competentes, y viceversa. d) Entre los CSIRT de referencia, y entre éstos y los CSIRT designados en otros Estados miembros de la Unión Europea. e) Entre los CSIRT de referencia y otros CSIRT nacionales o internacionales. f) Entre el punto de contacto único y los puntos de contacto únicos de otros Estados miembros de la Unión Europea. Los datos personales intercambiados se cancelarán cuando dejen de ser necesarios para la finalidad que motivó su cesión y, en todo caso, tras la notificación de cierre del incidente. Con posterioridad, los datos personales serán anonimizados.

Artículo 32. Supervisión de los operadores de servicios esenciales.
Artículo 33. Supervisión de los proveedores de servicios digitales.

Artículo 32. Supervisión de los operadores de servicios esenciales.

1. Las autoridades competentes podrán requerir a los operadores de servicios esenciales para que les proporcionen toda la información necesaria para evaluar la seguridad de las redes y sistemas de información, incluida la documentación sobre políticas de seguridad.
Podrán requerirles información sobre la aplicación efectiva de su política de seguridad, así como auditar o exigir al operador que someta la seguridad de sus redes y sistemas de información a una auditoría por una entidad externa, solvente e independiente.

2. A la vista de la información recabada, la autoridad competente podrá ordenar al operador que subsane los incumplimientos detectados e indicarle cómo debe hacerlo.

Artículo 33. Supervisión de los proveedores de servicios digitales.

1. La autoridad competente para la supervisión de los servicios digitales sólo inspeccionará el cumplimiento de las obligaciones derivadas de esta ley cuando tenga noticia de algún incumplimiento por petición razonada de otros órganos o denuncia. En tal caso, la autoridad competente podrá requerirle para que le proporcione toda la información necesaria para evaluar la seguridad de las redes y sistemas de información, incluida la documentación sobre políticas de seguridad, y para que subsane los incumplimientos detectados.

2. Cuando la autoridad competente tenga noticia de incidentes que afecten de modo significativo a servicios digitales ofrecidos por proveedores establecidos en España en otros Estados miembros, adoptará las medias de supervisión pertinentes. A estos efectos, tendrá especialmente en cuenta la información facilitada por las autoridades competentes de otros Estados miembros.

Se considera que la información requerida por las autoridades se debe referir al ámbito de esta Ley, no a la política general de la empresa, que pertenece al ámbito de la libertad de empresa.

Por ello, se propone ajustar el artículo 32.1:

1. *Las autoridades competentes podrán requerir a los operadores de servicios esenciales para que les proporcionen toda la información necesaria para evaluar* ***el cumplimiento de los requisitos necesarios para garantizar*** *la seguridad de las redes y sistemas de información, j****unto con la garantía y el secreto de las comunicaciones. Las autoridades competentes podrán inspeccionar los operadores sujetos a esta Ley para garantizar su cumplimiento, ~~incluida la documentación sobre políticas de seguridad~~***

El regulador se atribuye un derecho ilimitado de auditoria sobre operadores, tanto en número de auditorías exigibles como en profundidad de las mismas. Sobre los prestadores

de servicios digitales, el derecho es ilimitado en profundidad, dado que debe ser iniciado por denuncia.

Por otra parte, el regulador no contempla el reúso de la información derivada del programa de auditorías que operador o prestador ya estarán ejecutando en cumplimiento de 15.4.d.

La habilitación del ejercicio del derecho de auditoría por parte de las autoridades competentes es necesario para el buen desempeño de sus funciones. No obstante, el ejercicio de este derecho supone un sobrecoste para operadores, por lo que la limitación de los derechos de auditoría por el regulador aporta seguridad a los operadores y prestadores de servicio.

Por la misma razón, deben valorarse positivamente y reforzarse las acciones que permitan ejercer este derecho de forma efectiva con menores costes.

Se propone modificar el epígrafe 32.2, sobre reúso de información de auditoría, con el siguiente texto:

"El operador de servicios esenciales podrá sustituir la realización de auditorías por la aportación de la información recopilada en los últimos doce meses durante su programa de auditoría ejecutado de acuerdo con el artículo 15.4.d. A la vista de la información recabada, la autoridad competente podrá ordenar al operador que subsane los incumplimientos detectados e indicarle cómo debe hacerlo"

Se propone agregar el epígrafe 33.3:

"Las autoridades competentes ejercitarán este derecho de inspección y supervisión sobre operadores de servicios esencial como máximo con frecuencia anual"

Se propone modificar el epígrafe 33.2, sobre reúso de información de auditoría, con el siguiente texto:

"El proveedor de servicios digitales podrá sustituir la realización de auditorías por la aportación de la información recopilada en los últimos doce meses durante su programa de auditoría ejecutado de acuerdo con el artículo 15.4.d.
Cuando la autoridad competente tenga noticia de incidentes que afecten de modo significativo a servicios digitales ofrecidos por proveedores establecidos en España en otros Estados miembros, adoptará las medias de supervisión pertinentes. A estos efectos, tendrá especialmente en cuenta la información facilitada por las autoridades competentes de otros Estados miembros."

Artículos 38. Graduación de la cuantía de las sanciones
El órgano sancionador establecerá la sanción teniendo en cuenta los siguientes criterios: *a) El grado de culpabilidad o la existencia de intencionalidad.* *b) La continuidad o persistencia en la conducta infractora.* *c) La naturaleza y cuantía de los perjuicios causados.*

d) La reincidencia, por comisión en el término de un año de más de una infracción de la misma naturaleza cuando así haya sido declarado por resolución firme en vía administrativa. *e) El número de usuarios afectados.* *f) El volumen de facturación del responsable.* *g) La utilización por el responsable de programas de recompensa por el descubrimiento de vulnerabilidades en sus redes y sistemas de información.* *h) Las acciones realizadas por el responsable para paliar los efectos o consecuencias de la infracción.*
Se cita como atenuante el establecimiento de programas de recompensa por el descubrimiento de vulnerabilidades, pero no valora como tal el establecimiento de un proceso de gestión de vulnerabilidades, mucho más extendido en la actualidad y de mucha mayor eficiencia. Tampoco se hacen mención a otras medidas preventivas, tales como la concienciación de personal, o la imprevisibilidad del incidente, si responde a un incidente de seguridad conocido o un Zero-day. Ninguna organización puede asegurar que sus sistemas son 100% seguros, pero si debe exigirse haber tomado las medidas preventivas adecuadas (formación u otras). Asimismo, tampoco puede culpabilizarse a una organización de haber sido escogida como primer target por atacantes que dispongan de vulnerabilidades Zero-day. Si no se declara este eximente, la organización podría tener una triple penalización: sufrir una incidencia, dedicación de recursos a su rápida resolución y, adicionalmente, una cuantiosa sanción ante la que no ha podido tomar ninguna acción que la evitase. **Se propone modificar el artículo 38.g, con la siguiente redacción:** "La utilización por el responsable de programas de gestión de vulnerabilidades técnicas o de recompensa por el descubrimiento de vulnerabilidades en sus redes y sistemas de información." **Se propone añadir el epígrafe 38.i, con la siguiente redacción:** "la disponibilidad de información previa sobre las causas que han provocado el incidente y la imposibilidad de haber tomado medidas preventivas por desconocimiento de las mismas"

Artículo 39. Moderación de sanciones. **Artículo 40. Infracciones de las Administraciones públicas.**
Artículo 39. Moderación de sanciones. *1. El órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate, en los siguientes supuestos:* *a) Cuando se aprecie una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho como consecuencia de la concurrencia significativa de varios de los criterios enunciados en el artículo 38.*

b) Cuando la entidad infractora haya regularizado la situación irregular de forma diligente.
c) Cuando el infractor haya reconocido espontáneamente su culpabilidad.
d) Cuando se haya producido un proceso de fusión por absorción y la infracción fuese anterior a dicho proceso, no siendo imputable a la entidad absorbente.

2. Los órganos con competencia sancionadora, atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos en el apartado anterior, podrán acordar no iniciar la apertura del procedimiento sancionador y, en su lugar, apercibir al sujeto responsable, a fin de que en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que, en cada caso, resulten pertinentes, siempre que concurran los siguientes presupuestos:

a) Que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en esta ley.
b) Que el órgano competente no hubiese sancionado o apercibido con anterioridad al infractor como consecuencia de la comisión de infracciones previstas en esta ley.

Si el apercibimiento no fuera atendido en el plazo que el órgano sancionador hubiera determinado, procederá la apertura del correspondiente procedimiento sancionador por dicho incumplimiento.

3. No podrán ser objeto de apercibimiento las infracciones leves descritas en el artículo 36.4 c), d) y e) y la infracción grave prevista en el artículo 36.3 e).

Artículo 40. Infracciones de las Administraciones públicas

1. Cuando las infracciones a que se refiere el artículo 36 fuesen cometidas por órganos o entidades de las Administraciones Públicas, el órgano sancionador dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al órgano o entidad infractora y a los afectados, si los hubiera.

Además de lo anterior, el órgano sancionador podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran.

2. Se deberán comunicar al órgano sancionador las resoluciones que recaigan en relación con las medidas y actuaciones a que se refiere el apartado anterior.

El régimen sancionador establecido se centra en sanciones meramente económicas, de efecto disuasorio en el mejor de los casos. El montante de las sanciones económicas establecidas puede inducir a que se perciban con un fin recaudatorio, más que disuasorio. En particular, cuando las administraciones públicas no tienen establecida sanción económica alguna.

Asegurar que las sanciones económicas se destinan a la mejora de la seguridad del afectado por el incidente resultará en una mayor efectividad en la aplicación de la regulación y en un mejor servicio al ciudadano.

Se propone añadir un nuevo epígrafe 39.3 con el texto siguiente:

"El órgano sancionador podrá sustituir la imposición de la sanción económica al infractor, por la exigencia de dedicación en un plazo inferior a tres meses de presupuesto adicional igual al volumen de la sanción propuesta, destinado a la mejora de la seguridad de la organización"

Se propone añadir un nuevo epígrafe 40.3. con el texto siguiente:

"El órgano sancionador podrá requerir de la Administración Pública de la dedicación en un plazo inferior a tres meses de presupuesto adicional igual al volumen de la sanción que de la que hubiera sido objeto la Administración en caso no tratarse de un organismo público, destinado a la mejora de la seguridad de la organización. Este presupuesto deberá ser dedicado por la Administración del que tuviera actualmente asignado. El cambio de asignación presupuestaria deberá ser aprobado por los órganos de inspección e intervención oportunos"

Artículo 41. Competencia sancionadora.

1. La imposición de sanciones corresponderá, en el caso de infracciones muy graves, al Ministro competente en virtud de lo dispuesto en el artículo 9, y en el caso de infracciones graves y leves al órgano de la autoridad competente que se determine mediante el reglamento de desarrollo de esta ley.

2. La potestad sancionadora se ejercerá con arreglo a los principios y al procedimiento previsto en las Leyes 39/2015, de 1 de octubre, del procedimiento administrativo común de las Administraciones públicas, y 40/2015, de 1 de octubre, de régimen jurídico del sector público.

Existen varios órganos sancionadores, de acuerdo con las distintas autoridades competentes descritas en el artículo 9.

Añadir un mecanismo de supervisión y consistencia en las sanciones impuestas, haciendo que deban ser validadas por el Punto único de contacto del artículo 13, dará consistencia al régimen sancionador

Se propone añadir un epígrafe 41.3, con la siguiente redacción:

"Todas las sanciones muy graves y graves deberán ser aprobadas por el Punto Único de contacto designado por el artículo 13. El Punto Único de contacto tendrá potestad de variar la sanción impuesta para homogeneizarla con otras sanciones similares que hubiesen sido impuestas anteriormente"