La evaluación y la revisión de la Directiva NIS: la Directiva NIS 2.0

Félix Arteaga | Investigador principal, Real Instituto Elcano.

Tema

La Comisión Europea ha propuesto revisar la Directiva NIS, elaborada para armonizar las medidas de ciberseguridad de las redes y sistemas de comunicación, tras su evaluación durante 2020.

Resumen

La Comisión aprobó en julio de 2016 la Directiva NIS para mejorar la prevención y resiliencia de las redes y sistemas de comunicación públicos y privados de la UE dentro del Mercado Digital Único. La armonización prevista chocó con la diversidad de las normas de transposición y, sobre todo, de las medidas para implantar los objetivos previstos. Este ARI resume los antecedentes de su elaboración y describe los principales resultados de su evaluación y los cambios más importantes de la nueva propuesta.

Análisis

La Comisión aprobó en julio de 2016 la Directiva conocida como NIS[1] (*Security of Network and Information Systems*) para mejorar la prevención y resiliencia de las redes y sistemas de comunicación públicos y privados de la UE dentro del Mercado Digital Único. Con ella trató de armonizar las obligaciones de los operadores de servicios esenciales (OSE) y de los proveedores de servicios digitales (PSD) y obligar a los Estados miembros a elaborar estrategias, identificar autoridades NIS y disponer de equipos de respuesta a incidentes (CSIRT)[2]. Su elaboración comenzó en 2013, a pedido de la Estrategia de Ciberseguridad de 2013 y concluyó en 2016, tras un largo proceso de concertación con actores públicos y privados y un desigual grado de trasposición variable según los Estados miembros.

La Comisión tenía una visión instrumental de la ciberseguridad, porque la consideraba un medio necesario para alcanzar el fin de insertar la economía y la sociedad europeas en la economía digital. Bajo esta visión, la Comisión convocó también a los actores privados junto a los públicos a un mecanismo de coordinación transversal, el

[1] Directiva (UE) 2016/1148 de 6 de julio y Comunicación, COM(2017)476 y Anexo de 4 de octubre para armonizar su trasposición.

[2] Son operadores de servicios esenciales para la economía y la sociedad (OSE) los de la banca y el sector financiero, el transporte, la energía la salud y otros. Entre los proveedores de servicios digitales (PSD) figuran los relacionados con el comercio en línea, los servicios de computación en la nube o los motores de búsqueda.

denominado concepto plataforma[3] para asegurar que la Directiva atendía también a los intereses económicos en juego y no sólo a los intereses de ciberseguridad de las administraciones públicas.

La evaluación

La Directiva NIS preveía que la Comisión valorara su aplicación en mayo de 2021, pero la nueva Comisión decidió adelantar la revisión en su Programa de Trabajo 2020 a finales de año. Todo lo relacionado con lo digital (*Europe fit for the digital age*) había pasado a ser una de las prioridades de la Comisión junto con la sostenibilidad. Prioridades que se vieron reforzadas tras el impulso de la pandemia al proceso europeo de digitalización y ante el incremento constante de los ciberataques.

En julio de 2020 la Comisión reconocía en la Estrategia de la UE para una Unión de la Seguridad 2020-2025[4] la mayor relevancia de interconexión e interdependencia entre las infraestructuras físicas y las digitales poniendo de manifiesto la necesidad de un enfoque más coherente, uniforme y coordinado entre una propuesta de actualización de la Directiva para la protección y resiliencia de Infraestructuras Críticas[5] y la Directiva NIS 2.0.

Entre julio y octubre de 2020, la Comisión llevó a cabo una evaluación que tenía como objetivo comprobar si la seguridad de las redes y sistemas de información había mejorado o no, la relación entre costes y beneficios y los nuevos retos surgidos tras su entrada en vigor. La Comisión planteó las cuestiones a considerar, las opciones posibles de reforma y el calendario de evaluación en un documento para la Revisión de la Directiva NIS. En su opinión, la evaluación debería abordar la deficiente armonización debida a la discrecionalidad de los Estados miembros a la hora de trasponer y ejecutar la Directiva. Lo anterior perjudicaba a las empresas que operaban en distintos países y que tenían que seguir procedimientos distintos en cada uno de ellos. También tendría que evaluar la exclusión de algunos actores y sectores críticos para la economía digital, lo que creaba agravios comparativos y riesgos para las cadenas de suministro.

La consulta pública permitió la presentación de posiciones individuales de empresas o asociaciones. Entre ellas, la organización que agrupa a los operadores de móviles, GSMA, criticó la desigual trasposición y la necesidad de asegurar una mayor armonización, así como la simplificación de los procedimientos y la inclusión de suministradores de software o hardware para mejorar la eficacia de la Directiva. En sentido parecido, la asociación europea de redes de telecomunicaciones, ETNO, resaltó las dificultades que crea la desigual trasposición para empresas que operan en varios Estados miembros, por lo que era necesario reforzar la armonización, además de incluir a todos los proveedores de las cadenas de suministro y evitar los solapamientos

[3] Para una descripción de la interacción público-privada generada por este concepto, ver "Lecciones aprendidas durante la tramitación de la Directiva NIS", ARI 75/198 de 14 de julio de 2016.

[4] Comunicación COM (2020) 605 de la Comisión de 24 de julio sobre la Estrategia de la UE para una Unión de la Seguridad.

[5] Propuesta de Directiva COM (2020) 829 de la Comisión de16 de diciembre sobre resiliencia de las entidades críticas.

(inconsistencias) entre las distintas regulaciones sobre comunicaciones electrónicas, ciberseguridad e infraestructuras críticas[6].

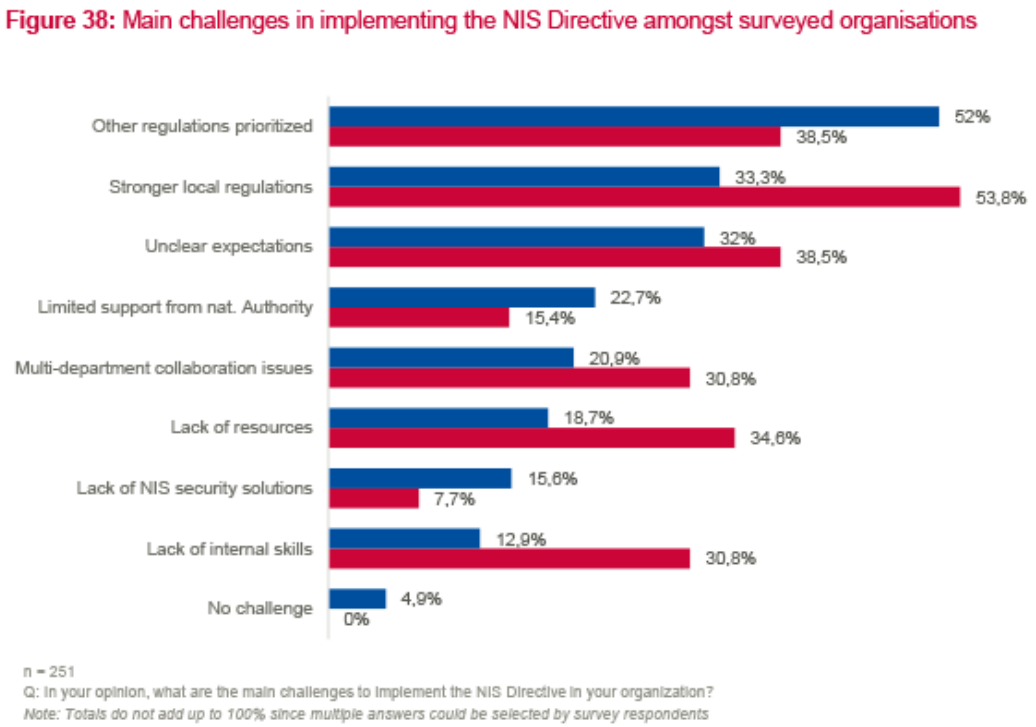
Por su parte, la Organización Europea de Consumidores, BEUC, reiteró la necesidad de forzar la armonización, para lo que sería mejor un Reglamento que una Directiva, así como la inclusión de los pequeños operadores y las plataformas de redes sociales. La Federación Europea de Banca, EBF, criticó la disparidad de los criterios de identificación de operadores de servicios esenciales en cada Estado miembro que conllevaba obligaciones diferentes en cada país y que imponía niveles de exigencia exagerados a algunos servicios bancarios. Finalmente, la Asociación Europea de Ciberseguridad, ECSO, se unió a las críticas por la desigual aplicación de la Directiva en las medidas de seguridad y la identificación de operadores realizada por cada Estado. Para remediarlo, se mostró partidaria de incluir a todos los eslabones de la cadena de suministro, incluidos los más pequeños; reforzar la armonización para crear un campo de juego más equilibrado; simplificar procedimientos como los de notificación de incidentes y fomentar la colaboración público-privada para incrementar el intercambio de información.

Dentro de la consulta, se circuló un cuestionario de evaluación de los efectos de la Directiva sobre los operadores y suministradores incluidos en ella y cuyos resultados figuran en un documento de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) [7] . Según la encuesta, 82% de las entidades consultadas valoraron positivamente el impacto de la Directiva sobre la seguridad. El impacto fue mayor en las áreas de gobernanza, riesgos y cumplimiento (64,5%), seguido de la seguridad de las redes (48,6%) y de la continuidad de negocios (33,1%) debido a la obligatoriedad de las obligaciones de cumplimiento y la de la declaración de incidentes. Otro porcentaje similar (80%) confirmó que estaban aplicando, total o parcialmente, sus medidas y un 64% reconoció haber adoptado medidas para detectar y comunicar incidentes, así como de concienciación y capacitación.

[6] La Comisión ha tenido en cuenta la consistencia de su propuesta en relación con la Directiva SWD (2019) 308 de 23 de julio sobre la resiliencia de entidades críticas o con la Directiva (2018) 1972 de 11 de diciembre sobre el Código Europeo de Comunicaciones Electrónicas, entre otras regulaciones.

[7] ENISA, "NIS Investments", diciembre 2020.

Figura 1. Principales retos para aplicar la Directiva



Fuente: ENISA, “NIS Investments”, p. 30.

En la Figura 1 se enumeran las principales dificultades encontradas por esas entidades a la hora de aplicar la Directiva. Varían según se hayan puesto en marcha planes de implantación (barras en azul) o se carezcan de ellos (barras en rojo). Las entidades más implicadas en la aplicación han encontrado dificultades para la coordinación con otras regulaciones en vigor prioritarias comunitarias o nacionales de ámbito transversal (ej. RGPD) o sectorial, así como la falta de claridad de las transposiciones nacionales. Por el contrario, la aplicación ha sido más difícil de poner en práctica en aquellas entidades que carecen de recursos, capacidad o coordinación[8].

Para las entidades españolas que participaron en la encuesta, las principales dificultades que han encontrado en la aplicación de la Directiva NIS serían, por este orden, la prioridad de normas como el RGPD (51,2%), la falta de claridad (32,6%), el limitado apoyo de las autoridades nacionales (27,9%), otras normas nacionales (23,3%) y la falta de recursos (18,6%), de coordinación (16,3%) o habilidades (14%).

[8] Los resultados no pueden extrapolarse al conjunto del sector de la ciberseguridad (sólo participaron en la encuesta 50 organizaciones españolas) pero los encuestados revelan una implantación del 48% frente a la media de 58.6%,

La revisión

Como resultado de lo anterior, la Comisión elaboró varios estudios de impacto que acompañan a la Propuesta para aumentar el nivel común de ciberseguridad de la UE[9]. En la parte inferior se encuentran los principales problemas detectados durante la evaluación: falta de cobertura, limitada claridad en el alcance y competencias, divergencias en las notificaciones, supervisión e imposición limitadas, desfase de recursos y escaso intercambio de información entre los Estados miembros.

Estas desviaciones se explican, entre otros, porque no todos los actores obligados adoptaron medias y otros se excluyeron de la obligación; la voluntariedad de la cooperación y la limitada armonización debida a la disparidad de transposiciones. Como resultado, no ha mejorado como se pretendía el nivel de resiliencia de economía de ciberseguridad, ni se ha armonizado de forma consistente y tampoco ha mejorado sensiblemente la conciencia colectiva de situación o la gestión de crisis colectiva. Lo que ha tenido consecuencias económicas, afectado a los servicios públicos, a la desconfianza digital y a un alto coste económico y operativo para las empresas que operan en los distintos países de la UE.

[9] Impact Assessment Proposal for directive on measures for high common level of cybersecurity across the Union. Comprende un sumario ejecutivo, uno estudio sobre las conclusiones de la evaluación y otros dos con los distintos anexos de la valoración de impacto.

Figura 2. Resumen de problemas, causas y consecuencias de la evaluación

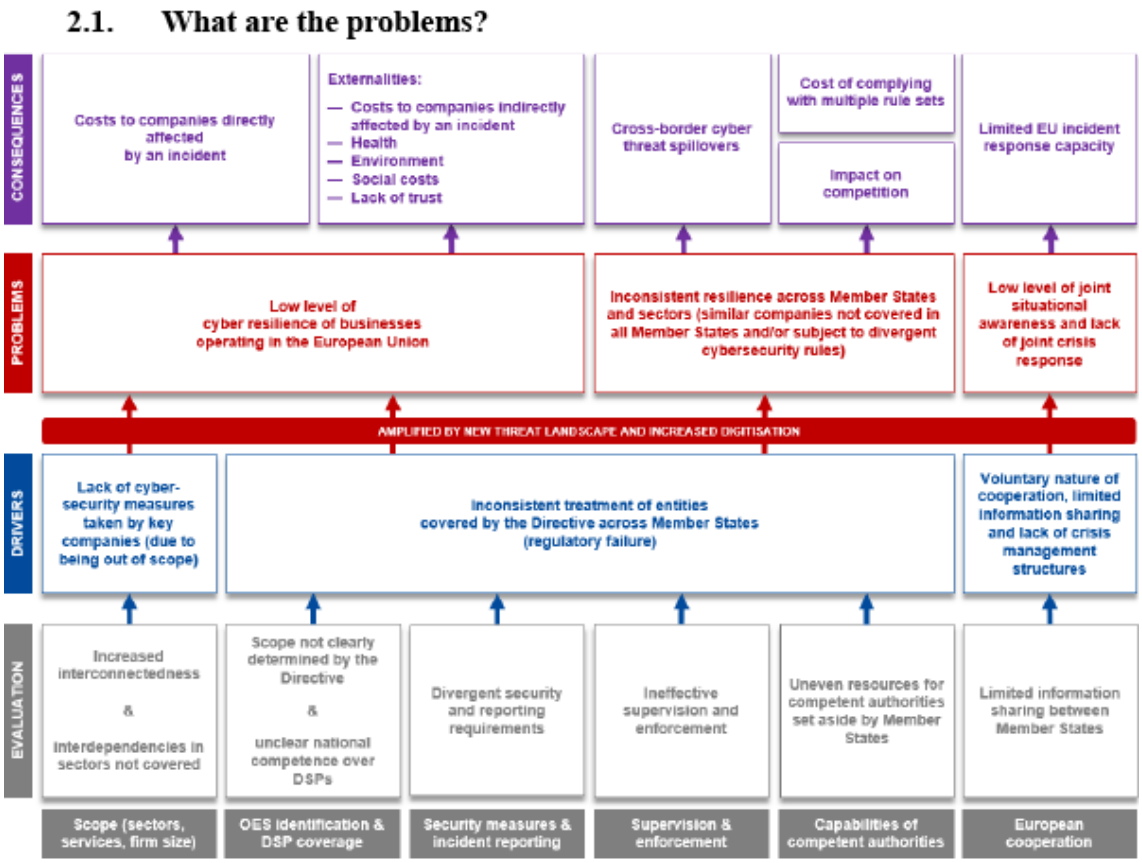


Figure 2: Outcome of the evaluation, problem drivers, problems and consequences

Fuente: Impact Assessment SWD (2020)345, parte 1/3, p. 15.

Como resultado de sus valoraciones y de las recabadas del sector durante la consulta pública, la Comisión presentó una propuesta de revisión[10] a la que se denomina en este artículo como Directiva NIS 2.0 sin que esa denominación cuente con respaldo oficial o consuetudinario de momento. Básicamente, la revisión trataba de mejorar algunos problemas que la Directiva NIS no había resuelto y que aparecían en la evaluación de su impacto mencionada anteriormente como la reducida ciberresiliencia empresarial, la diferente implementación según los países, el bajo conocimiento situacional y la carencia de respuestas comunes. La valoración de la Comisión coincidía con la del sector de los operadores esenciales que se veían perjudicados por el margen de discrecionalidad y la baja armonización de las regulaciones nacionales que penalizaba a los operadores frente a otros actores digitales no incluidos en la Directiva, por lo que pedían equilibrar el terreno de juego entre todos los actores.

[10] Propuesta de Directiva COM (2020) 823 final de la Comisión de 16 de diciembre sobre medidas para un alto nivel común de Ciberseguridad en la UE y Anexos sobre entidades esenciales e importantes.

En su exposición de motivos, la Comisión reconoce que:

- El ámbito de aplicación de la Directiva NIS se ha quedado pequeño debido al avance de la digitalización y la conectividad en los últimos años y no incluye a servicios digitales relevantes.

- Tampoco incluye a todos los actores relevantes porque los criterios de la Directiva y de las transposiciones nacionales para identificar los proveedores de servicios digitales no han sido claros.

- Por las mismas razones, el procedimiento para la notificación de incidentes por los proveedores de servicios esenciales no es el mismo y las sanciones y exigencia de obligaciones varía en cada Estado miembro.

- El intercambio de información entre actores públicos y privados sigue siendo muy bajo y poco sistematizado.

- La disparidad de los recursos presupuestarios y humanos disponibles por los Estados miembros condiciona su nivel de madurez y su capacidad de ciberresiliencia.

Para hacer frente a estos retos, y entre las distintas opciones barajadas[11], la Comisión ha optado por introducir cambios "sistémicos y estructurales" en relación con el ámbito, los actores, la armonización y la exigencia de las obligaciones. Una opción que en la evaluación del impacto se justifica porque, en su conjunto, las medidas pueden disminuir los costes asociados a los incidentes en unos 11.300 millones de euros. No obstante, la Propuesta se ha tramitado como una directiva en lugar de como un reglamento que hubiera forzado una mayor armonización.
Entre los nuevos actores se incluyen los suministradores de servicios o redes públicas de comunicación, los de contenidos o datos, los de plataformas de redes sociales y los dedicados a fomentar la confianza en los anteriores. Entre los nuevos sectores figuran las Administraciones Públicas, los servicios postales, la gestión de aguas, el espacio, la alimentación y ciertos productos críticos. Se han introducido medidas para institucionalizar un marco europeo en la gestión de crisis o asegurar las cadenas de suministro.

La Propuesta suprime la distinción entre OSE y PSD y establece, en su lugar, una diferenciación en función de su tamaño e importancia. Según el tamaño, la Comisión sólo incluye aquellas entidades que tienen un tamaño mediano y grande, salvo algunos supuestos tasados para tamaños inferiores[12]. Entre los incluidos, la Comisión discrimina entre las "entidades esenciales" que operan en sectores críticos (banca, energía,

[11] Según la Propuesta serían: 1) No hacer nada; 2) proponer recomendaciones no legislativas; 3) Proponer cambios puntuales y coyunturales a la Directiva y 4) elaborar una nueva Directiva.

[12] Los criterios de esta diferenciación por tamaño figuran en la Recomendación (2003) 361 de 6 de mayo sobre la definición de empresas de tamaño medio, pequeñas y micro. Estas dos últimas no entrarían en la nueva Directiva salvo los proveedores de equipos y servicios redes de comunicación electrónicas, pequeñas y de tamaño medio.

transporte, salud, infraestructuras digitales, agua, administración y espacio) y las "entidades importantes" que operan en sectores no tan críticos (alimentación, químicas, distribución, servicios digitales). Aunque los medianos y pequeños quedan excluidos del ámbito directo de aplicación, tendrán que hacer frente a las obligaciones derivadas de los cambios que les afecten.

Los Estados miembros deben supervisar las medidas que adoptan las entidades anteriores para prevenir los riesgos y que notifican los incidentes que afecten significativamente a los servicios que prestan. También deben cooperar con otros Estados cuando la entidad comparta sede en varios países. Deben hacerlo de dos formas distintas según se trate de entidades esenciales o importantes. En el primer caso, llevarán a cabo inspecciones y auditorias preventivas, mientras que en el segundo caso harán lo mismo sólo cuando existan evidencias notorias de incumplimiento. Las actuaciones podrían conllevar amonestaciones, instrucciones y multas de hasta 2 millones de euros o el 2% de los ingresos anuales. No se precisan las medidas, lo que deja un margen de flexibilidad a obligados y supervisores para fijarlas caso por caso bajo un enfoque de gestión de riesgos[13].

Para asegurarse del rendimiento de cuentas, se incrementa la responsabilidad de los órganos de dirección y de los gestores de la seguridad en la elaboración y ejecución de las medidas, así como de su capacitación profesional para hacerlo. A su vez, los Estados miembros se supervisarán entre ellos para medir periódicamente la eficacia de sus políticas de ciberseguridad[14]. La ampliación de la supervisión obligará a las administraciones públicas a reforzar sus medios (entre 20% y 30%) y a mantener una relación más estrecha con ellos. También tendrán que hacer un esfuerzo suplementario las grandes entidades, mayor para las nuevos implicados (22%) que para los que ya estaban supervisados (10%).

Conclusiones y pasos por dar

La Propuesta comenzará su trámite legislativo tras concluir en febrero de 2021 el último periodo de consulta pública para convertirse en la Directiva NIS 2.0 que abrirá, a su vez, los procesos nacionales de trasposición. Estos coinciden en España con la entrada en vigor del Reglamento que desarrolla la trasposición anterior[15].

El proceso de evaluación y revisión seguido para elaborar la nueva Propuesta de Directiva debería emularse en España para valorar el resultado de la transposición seguida y, en su caso, identificar los cambios necesarios para corregir los impactos negativos que se encuentren. Esta evaluación debería llevarse en paralelo con el estudio de las soluciones que presenta la Propuesta de Directiva NIS 2.0.

[13] Entre las medidas que se mencionan figuran algunas ya contempladas en la Directiva NIS como el análisis de riesgos, gestión de incidentes, continuidad de negocio o la gestión de crisis, y algunos nuevos como la seguridad en las cadenas de suministro y el uso de criptografía y cifrado. Art. 18.

[14] El procedimiento está pendiente de elaboración, pero la Propuesta pretende evaluar, al menos, las capacidades y recursos de las autoridades de ciberseguridad nacionales y la eficacia de sus CSIRT, de su asistencia mutua y del intercambio de información (art. 16).

[15] R.D. 43/2021 de 26 de enero que desarrolla el Real Decreto-ley 12/2018 de 7 de septiembre de seguridad de las redes y sistemas de información.

La emulación supone una mayor interlocución público-privada que no se restrinja, como hasta ahora, a un período limitado de consulta pública. La creación del Foro de Ciberseguridad Nacional permite recrear el concepto plataforma adoptado por la Comisión para que el Gobierno tenga en cuenta la opinión y el impacto de su adaptación legislativa sobre los actores y sectores implicados desde el inicio del proceso.