DIGITALEUROPE

Transposición de la Directiva sobre seguridad de las redes y de la información (NIS)

Bruselas, 5 Julio 2016

DOCUMENTO DE SÍNTESIS

El Consejo de la Unión Europea publicó la versión definitiva de la Directiva sobre seguridad de las redes y de la información (NIS) el 21 de abril de 2016. Si bien esta debe ser oficialmente aprobada por el Parlamento Europeo este verano, el texto en sí ya ha sido acordado por las tres instituciones europeas y no se prevé que sufra modificaciones. Los Estados miembros tendrán que transponerla en su legislación nacional en un plazo de 21 meses tras su adopción. Al objeto de colaborar en este proceso, adjuntamos como apéndice una guía de mejores prácticas para implementar los aspectos relevantes para la industria tecnológica y preservar de forma eficaz las intenciones de los autores del borrador.

La Directiva europea NIS, la primera ley paneuropea sobre ciberseguridad, se centra en reforzar el papel de las ciberautoridades a escala nacional, intensificando la coordinación entre estas e introduciendo requisitos de seguridad para los sectores industriales clave.

Ninguna de las leyes de ejecución nacionales debe obviar los dos objetivos principales de la Directiva: (1) garantizar un elevado nivel de ciberseguridad de las infraestructuras críticas del país; (2) el establecimiento de un mecanismo de cooperación eficaz entre los Estados miembros de la UE para favorecer el logro de esta meta. Los recursos deben dedicarse principalmente a la consecución de estos dos importantes objetivos.

En el caso de la industria tecnológica, las disposiciones relativas a los denominados proveedores de servicios digitales (DSP) revisten especial interés. La Directiva pone de manifiesto claramente que existen diferencias fundamentales entre los operadores de servicios esenciales (OES) y los DSP. De hecho, estos últimos no deben ser considerados una infraestructura crítica como tal. Tal y como reconoce la legislación, un incidente que afectase a estos servicios digitales representaría un nivel de riesgo considerablemente inferior para la seguridad económica y pública de un país. El mantenimiento de esta distinción es esencial para poder desplegar de forma eficaz los escasos recursos de las autoridades que tendrán que supervisar y velar por el cumplimiento de las normas.

En consecuencia, recomendamos prestar especial atención al ámbito de aplicación previsto para los servicios en cuestión y solicitamos a los responsables políticos que no impongan los requisitos de seguridad a sectores distintos de los identificados como DSP y OES en la legislación nacional.

En lo que respecta a la jurisdicción, los DSP deberán poder acogerse a la legislación vigente en el país de su establecimiento principal, incluso en aquellos casos en los que estén involucradas las autoridades competentes de varios países. En lo referente a la supervisión, las autoridades competentes deberán seguir un enfoque a posteriori en lugar de imponer una obligación general de vigilancia de los DSP. Es más, deberán centrarse en los resultados y mantener la distinción entre los OES y los DSP, no sometiendo a estos últimos a los requisitos no previstos por la Directiva, como auditorías e instrucciones vinculantes.

DIGITALEUROPE
Rue de la Science, 14 - 1040 Bruselas [Bélgica]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Miembro del Registro de Transparencia para la Comisión: 64270747023-20

Las medidas de seguridad impuestas a los DSP deberán diferir de las de los OES, dado que la Directiva establece que estos representan un riesgo para la seguridad considerablemente menor. Los responsables de la toma de decisiones deberán materializar la armonización de estos servicios, reconocer los estándares internacionales ya existentes promovidos por la industria, evitar los mandatos tecnológicos y respetar el derecho de los DSP (protegido por la Directiva) a definir las medidas de seguridad más adecuadas para sus sistemas. Los mecanismos de notificación de incidentes también deben, en la medida de lo posible, armonizarse a escala europea, centrarse en los incidentes que afecten a la continuidad del servicio, respetar la flexibilidad en los plazos de notificación y crear un entorno seguro que favorezca la comunicación de información sin exponer a la parte notificante a una mayor responsabilidad

Las medidas impuestas a los OES también afectarán a otros sectores, ya que las medidas de seguridad y las obligaciones de notificación de incidentes se trasladarán en las disposiciones contractuales. Esto es particularmente crucial en los servicios en nube. En consecuencia, puede que los DSP se vean sujetos de manera indirecta a la legislación nacional de sus clientes y que, por lo tanto, tenemos especialinterés en que las medidas de seguridad internacionalmente reconocidas sean aplicadas a estos servicios. También proponemos, en la medida de lo posible, medidas de coordinación y sinergias entre los requisitos de notificación tanto para los OES como para los DSP, dado que es probable que estos últimos se vean sujetos a una obligación de notificación doble.

La Directiva establece como meta conseguir un elevado nivel de seguridad común en las redes y los sistemas de información con objeto de mejorar el funcionamiento del mercado interno. Para lograr este ambicioso objetivo, las transposiciones nacionales deben centrarse en un enfoque internacional y armonizado basado en el riesgo que proporcione a los actores del sector privado la flexibilidad necesaria para adaptarse a un panorama de amenazas en constante cambio, que permita a las ciberautoridades destinar sus limitados recursos a los problemas más importantes y que reconozca que la solución a un problema sin fronteras tiene que ser global. Esperamos que esta guía sea una herramienta útil para la consecución de este fin y estaremos encantados de responder a las dudas que pueda suscitar.

Apéndice: Guía sobre mejores prácticas para la implementación de la Directiva NIS

1. Proveedores de servicios digitales

a) Ámbito

- La Directiva determina que los mercados en línea, los motores de búsqueda en línea y los servicios de computación en nube deben considerarse proveedores de servicios digitales (DSP) y, en consecuencia, incluirse en el ámbito de aplicación de la Directiva. Si bien se trata de una Directiva de armonización mínima (Artículo 2), es importante mantener la coherencia en toda la UE y, en consecuencia, los Estados miembros no deben imponer los requisitos de seguridad a sectores distintos de los identificados como DSP u operadores de servicios esenciales (OES), según la definición del Artículo 3, en la legislación nacional.

- La Directiva establece de manera explícita que los fabricantes de hardware y los desarrolladores de software no son OES ni DSP, por lo que no deben estar sujetos a las leyes nacionales que implementen la Directiva (Considerando 50).

- La Directiva excluye del ámbito de aplicación de manera explícita los servicios de los mercados en línea que actúan como intermediarios de servicios terceros en los que el contrato de venta o servicio se concluye en última instancia (por ejemplo, sitios de comparación) (Considerando 15).

- Las funciones de búsqueda limitadas al contenido de un sitio web concreto no deben quedar incluidas como motores de búsqueda en línea aunque recurran a un proveedor externo (Considerando 16).

- La definición de un servicio de computación en nube de conformidad con la Directiva depende de los recursos de computación que sean compartidos por múltiples usuarios (Artículo 4(19) y Considerando 17). Dado que las nubes privadas (a diferencia de las nubes públicas) se dedican a una única organización, no deben ser incluidas.

- La Directiva subraya que existen diferencias fundamentales entre los OES y los DSP, y por este motivo los DSP están sujetos a normas distintas (Considerando 57). Esta distinción deberá mantenerse cuando se implemente la Directiva.

b) Jurisdicción y supervisión

- La jurisdicción sobre los DSP deberá atribuirse a un único Estado miembro, aquel en el que el operador tenga su establecimiento principal dentro de la UE. Este corresponderá, en principio, al lugar donde se encuentre su sede central en la UE (Artículo 18.1 y Considerando 64). Sostenemos que deben ser los DSP quienes determinen esto y que esta decisión únicamente podrá modificarse en caso de que las autoridades competentes la cuestionen en el contexto de actividades de supervisión a posteriori.

- En caso de que los DSP dispongan de redes y sistemas de información en países distintos del de la ubicación de su establecimiento principal, el Artículo 17.3 prevé la colaboración de las autoridades competentes. Sin embargo, desde el punto de vista de los DSP, es importante que la legislación aplicable siga siendo la del país de su establecimiento principal y que sigan siendo exclusivamente responsables ante la autoridad competente en dicha jurisdicción, quien actuará como su interlocutor.

- La Directiva pone de relieve que los DSP están sujetos a una supervisión a posteriori reactiva y, en consecuencia, las autoridades competentes no tienen ninguna obligación general de supervisar a los DSP y únicamente deben actuar si tienen pruebas. (Artículo 17.1 y Considerando 60). Estas disposiciones deberán respetarse cuando se implemente la Directiva.

- A diferencia de los OES, en el caso de los DSP, las autoridades únicamente pueden solicitar información y exigir a los DSP que subsanen cualquier fallo. La Directiva establece claramente que las autoridades no poseen competencias de auditoría y no pueden emitir instrucciones vinculantes. Estas disposiciones también deberán respetarse a escala nacional.

c) Requisitos adicionales

- Los requisitos de seguridad y notificación impuestos a los DSP serán objeto de una armonización máxima (Artículo 16.10). Deberá considerarse que este Artículo se aplica a los productos, servicios y soluciones que conforman sus redes y sistemas de información. En consecuencia, disposiciones adicionales, como las pruebas de productos, no deberán exigirse en la medida en la que los productos y servicios se utilicen en este contexto.

d) Estándares y medidas de seguridad

- Las medidas de seguridad para los DSP deberán ser menos estrictas que para los OES. Los DSP deberán disponer de libertad para definir el modo de aplicar las medidas de seguridad y de garantizar la protección de su red y sistemas de información de una forma adecuada a los riesgos planteados (Considerando 49).

- Las medidas de seguridad deberán estar orientadas a los procesos y centrarse en la gestión del riesgo. No deberán exigir que los productos TIC se diseñen, desarrollen o fabriquen de un modo concreto (Considerando 51).

- La Directiva hace hincapié en el hecho de que los Estados miembros no podrán imponer ningún requisito de seguridad adicional a los DSP (Artículo 16.10).

- No obstante, esperamos pautas de múltiples actores. Los Estados miembros garantizarán la adopción de las medidas dispuestas en la Directiva (Artículo 16.1). En este sentido, podrán promover la aplicación de estándares para implementarlas (Artículo 19.1) y debatir estos estándares con los organismos europeos de normalización del Grupo de cooperación (Artículo 11.3(h)). ENISA les ofrecerá asesoramiento sobre los estándares adecuados (Artículo 19.2) y la Comisión Europea se encargará de adoptar actos de ejecución sobre las medidas de seguridad (Artículo 16.8).

- Dado este nivel de complejidad y las ventajas de la armonización, recomendamos quelos procesos nacionales, en esencia, se aplacen a los actos de ejecución para acordar medidas adecuadas que, en cualquier caso, tendrán que completarse en un plazo de un año tras la adopción de la Directiva. Los actos de ejecución deberán aplicarse sin perjuicio de la capacidad de los DSP de definir las medidas de seguridad más adecuadas para sus sistemas.

- El Artículo sobre los estándares permite remitirse a los estándares europeos o internacionalmente aceptados (Artículo 19.1). Dada la madurez de los estándares internacionales aplicados en este campo, recomendamos que, en caso de que existan estándares adecuados, baste con la certificación conforme a uno de ellos (como ISO 27001) para cumplir los requisitos.

- En cualquier caso, la certificación según estándares deberá ser opcional y no obligatoria. El Artículo 19 establece que los estándares únicamente se podrán «fomentar» y que esto deberá hacerse «sin imponer ni favorecer el uso de un tipo específico de tecnología».

e) Notificación de incidentes de seguridad

- Al igual que ocurre con las medidas de seguridad, son varias las partes que participan en la determinación del mecanismo de notificación de incidentes de conformidad con la Directiva NIS. Los Estados miembros tienen que garantizar que los DSP notifiquen los incidentes de seguridad con repercusiones importantes sobre la prestación del servicio (dentro del ámbito de aplicación de la Directiva) que presten (Artículo 16.3). El Grupo de cooperación estará a cargo de debatir las modalidades de notificación (Artículo 11.3(m)) y la Comisión adoptará los actos de ejecución (Artículos 16.8 y 9).

- De nuevo, recomendamos que en las transposiciones nacionales el proceso se defiera a los actos de ejecución, de los cuales, el acto de ejecución sobre el límite para la notificación deberá adoptarse en un plazo de un año tras la compleción de la Directiva.

- En lo que respecta a los tipos de incidentes que deben notificarse, los DSP deberá comunicar «cualquier incidente que tenga un impacto significativo en la prestación de [su] servicio» (Artículo 16.3). En lo referente a la implementación de las disposiciones equivalentes para los operadores de telecomunicaciones de conformidad con el marco del Artículo 13a de la Directiva, creemos que debe interpretarse que esta se centra en la continuidad (o disponibilidad) de los servicios prestados. En otras palabras, los casos de indisponibilidad que lleguen a un nivel concreto (pendiente de determinación mediante los actos de ejecución) deberán notificarse antes que cualquier otro tipo de incidente de seguridad. Esto permitirá centrarse en los incidentes con mayores probabilidades de afectar a la economía o a la sociedad, minimizando (aunque sin erradicar por completo) el solapamiento con los requisitos de notificación de infracciones en relación con los datos personales previstos en el Reglamento general de protección de datos.

- Además, la obligación de notificación para los «operadores de servicios esenciales» especifica que estos notificarán los «incidentes que tengan efectos significativos en la continuidad de los servicios que prestan», de nuevo con una clara orientación a la continuidad (o disponibilidad) del servicio. Los colegisladores acordaron que las obligaciones impuestas a los DSP deberán ser menos estrictas que las de los OES (véase el Considerando 49). La obligación de notificación de incidentes de los DSP de

conformidad con NIS no deberá ser más amplia que la de los OES; de hecho, debería adaptarse con mayor precisión en lo que a los límites respecta. Esto subraya nuevamente que la notificación de incidentes por parte de los DSP deberá limitarse a los incidentes que alcancen un límite concreto y que **afecten a la continuidad/disponibilidad del servicio**, quedando excluidos los incidentes relativos a la integridad o la confidencialidad de los datos, un aspecto que, en gran medida, ya está cubierto por los requisitos de notificación relacionados previstos en los reglamentos GDPR y eIDAS.

- En lo referente a los plazos de notificación, valoramos la flexibilidad implícita en la expresión «sin dilación indebida» (Artículo 16.3). La implementación no deberá dar lugar a plazos estrictos, ya que la complejidad de los incidentes puede variar considerablemente. Unos plazos de notificación uniformes darían lugar a comunicaciones imprecisas en las que el ámbito de aplicación inicial de los sistemas implicados no estaría claro y afectaría a la capacidad de los profesionales de respuesta a incidentes de dar prioridad a la reacción ante el incidente frente a su notificación.

- Como ya se ha señalado, puede que los incidentes de seguridad que deben notificarse de conformidad con la Directiva también tengan que comunicarse según lo dispuesto en la ley de protección de datos, en función de si se ha producido una infracción en relación con datos personales. Esto no solo implica notificar el mismo incidente a distintas autoridades, sino que puede incluso que estas autoridades se encuentren en Estados miembros diferentes en función de la jurisdicción aplicable al DSP de conformidad con las dos leyes. Recomendamos que los Estados miembros reconozcan la necesidad y eviten la duplicación de las notificaciones de incidentes tratando de crear canales de comunicación para compartir información relevante entre ellos sin perjuicio de la confidencialidad empresarial.

- Las autoridades competentes deberán tener en cuenta las implicaciones comerciales y para la imagen de los DSP antes de divulgar información sobre incidentes públicamente. Y lo que es más importante, la revelación del incidente podría incrementar el riesgo para la seguridad. Por lo tanto, es importante la coordinación con los actores en cuestión previamente a cualquier divulgación.

- La Directiva hace hincapié en que la información que se considera confidencial deberá tratarse como tal (Considerandos 41, 59, Artículo 1.5).

- El Artículo 16.3 establece que la notificación de los incidentes de seguridad no deberá exponer a la parte notificante a una mayor responsabilidad.

2. Operadores esenciales

a) Responsabilidad solidaria sobre las medidas de seguridad

- Los DSP, que tengan OES como clientes, estarán sujetos a aquellas medidas de seguridad aplicables derivadas de las obligaciones estatutarias impuestas a los operadores esenciales (Artículo 14.1) que se plasmen en las negociaciones contractuales. En consecuencia, puede que se vean indirectamente sujetos a la legislación nacional de sus clientes, con independencia de la legislación vigente en el país de su sede central en Europa.

- Como resultado, las medidas para armonizar las medidas de seguridad impuestas a los operadores esenciales serían bien acogidas. Si bien los Estados miembros tienen derecho a imponer obligaciones más estrictas sobre los operadores esenciales que las previstas por la Directiva (Artículo 3), recomendamos moderación en este sentido y animamos a los Estados miembros a que busquen un enfoque armonizado. Esto se puede lograr evitando medidas adicionales en las transposiciones nacionales y se trata de determinar las medidas de seguridad adecuadas en el Grupo de cooperación en lugar de centrarse en el proceso nacional.

- En la medida de lo posible, los requisitos de seguridad deberán basarse en estándares internacionales (como los de la serie ISO 27x) y en mejores prácticas de seguridad reconocidas.

- Las medidas de seguridad impuestas a los OES no deberán requerir en ningún caso que productos TIC concretos se diseñen, desarrollen o fabriquen de un modo específico (Considerando 51).

b) Responsabilidad solidaria sobre la notificación de incidentes de seguridad

- Los operadores de servicios esenciales estarán obligados a notificar los incidentes de seguridad que afecten a la continuidad de sus servicios esenciales que se produzcan en sus DSP contratados (Artículo 16.5). Por lo tanto, se exigirá a los DSP por contrato que notifiquen al operador esencial en cuestión aquellos incidentes de seguridad que pudieran afectarles.

- Valoramos la flexibilidad en los plazos de notificación para los OES inherente a la expresión «sin dilación indebida» (Artículo 14.3). Las transposiciones nacionales no deberán incorporar plazos específicos y, en cualquier caso, si se solicita a los OES que justifiquen el tiempo empleado en la notificación, el periodo en cuestión deberá contarse desde el momento en el que el incidente llegue a conocimiento del OES, no desde el momento en el que llegue a conocimiento del DSP.

- El Artículo 14.7 prevé la redacción por parte del Grupo de cooperación de unas pautas sobre las circunstancias para la notificación frente al papel armonizador de la Comisión para las notificaciones de los DSP. Dada la duplicación de los requisitos de notificación para los DSP, es importante que los respectivos requisitos de notificación no sean contradictorios y estén armonizados en la medida de lo posible. Por lo tanto, este proceso deberá revisarse para orientarlo hacia la consecución de este objetivo. Es más, los requisitos de notificación para los DSP deberán respetar las obligaciones de confidencialidad contraídas con sus clientes OES y no exigirles que compartan información empresarial confidencial.

ACERCA DE DIGITALEUROPE

DIGITALEUROPE representa a la industria de la tecnología digital en Europa. Entre nuestros miembros se incluyen algunas de las empresas de TIC, telecomunicaciones y electrónica de consumo más importantes del mundo, así como asociaciones nacionales de todas partes de Europa. DIGITALEUROPE trabaja para que las empresas y ciudadanos europeos se beneficien plenamente de las tecnologías digitales y atraer y apoyar a las mejores empresas de tecnología digital del mundo para que Europa crezca.

DIGITALEUROPE garantiza la participación de la industria en el desarrollo e implementación de las políticas europeas. Los miembros de DIGITALEUROPE incluyen 62 miembros corporativos y 37 asociaciones profesionales nacionales de toda Europa. Nuestra página web contiene información adicional sobre nuestras últimas noticias y actividades: http://www.digitaleurope.org

MIEMBROS DE DIGITALEUROPE

Miembros corporativos

Airbus, Amazon Web Services, AMD, Apple, BlackBerry, Bose, Brother, CA Technologies, Canon, Cisco, Dell, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Ingram Micro, Intel, iQor, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Samsung, SAP, SAS, Schneider Electric IT Corporation, Sharp Electronics, Siemens, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, Zebra Technologies, ZTE Corporation.

Asociaciones nacionales de comercio

Austria: IOÖ
Bielorrusia: INFOPARK
Bélgica: AGORIA
Bulgaria: BAIT
Chipre: CITEA
Dinamarca: DI Digital, IT-BRANCHEN
Estonia: ITL
Finlandia: FFTI
Francia: AFNUM, Force Numérique, Tech in France
Alemania: BITKOM, ZVEI
Grecia: SEPE
Hungría: IVSZ
Irlanda: ICT IRELAND
Italia: ANITEC
Lituania: INFOBALT
Países Bajos: Nederland ICT, FIAR
Polonia: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Rumanía: ANIS, APDETIC
Eslovaquia: ITAS
Eslovenia: GZS
España: AMETIC
Suecia: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Suiza: SWICO
Turquía: Digital Turkey Platform, ECID
Ucrania: IT UKRAINE
Reino Unido: techUK