CONTENIDO DE LA TRANSPOSICIÓN DE LA DIRECTIVA NIS 2: TEMAS PRIORITARIOS.

ANÁLISIS FLASH

VICENTE MORET

CRISTINA DURANTE

ESYS
EMPRESA SEGURIDAD Y SOCIEDAD DIGITAL

Marzo 2023

Calle de Caracas, 6, Planta Baja, 28010, Madrid.

Contacto

+34 914252577 /609484940

www.fundacionesys.com

ESYS
EMPRESA SEGURIDAD Y SOCIEDAD DIGITAL

ANÁLISIS FLASH

VICENTE MORET

Letrado de las Cortes Generales, abogado asesor en Andersen, experto en negociación ciber, profesor adjunto en IE Law School. Secretario del Patronato de la Fundación ESYS.

CRISTINA DURANTE

Associate en Andersen.

Marzo 2023

La trasposición de la Directiva NIS2 constituye un importante hito en términos de regulación de la seguridad digital en España. En este sentido, es una oportunidad para crear un completo, sólido y homogéneo marco de regulación que además resuelva algunas de las disfunciones que se han producido durante la vigencia del RD-ley 12/2018, y el RD 43/2021 que han integrado en el marco normativo español la regulación contenida en la Directiva NIS 1.

En este sentido, y de cara a llevar a cabo la trasposición, en este documento se proponen los temas prioritarios que deberían abordarse para la transposición de la Directiva NIS 2 al ordenamiento jurídico español antes del 17 de octubre de 2024.

1) Delimitación especifica del ámbito de aplicación por sectores y por volumen de las empresas obligadas.

- Se considera necesario definir de manera clara y detallada los sectores y el tamaño de las empresas que están obligadas a cumplir con NIS 2.

- Determinar el alcance de entidades obligadas en virtud del artículo 2.2.e) por ser consideradas críticas por su importancia específica a nivel nacional o regional para el sector o tipo de servicio concreto, o para otros sectores interdependientes, o por su importancia económica.

- Considerar la creación de un régimen diferente de obligaciones para las PYMES que resulten obligadas.

- Determinar si NIS 2 se aplicará a: a) entidades de la Administración pública a nivel local; y b) centros de enseñanza, en particular cuando lleven a cabo actividades críticas de investigación.

2) Conexiones del desarrollo normativo de esta norma junto con la Directiva de resiliencia de entidades críticas.

- Mecanismos de cooperación e intercambio de información entre las autoridades competentes de acuerdo con NIS 2 y las autoridades competentes de acuerdo con la Directiva de resiliencia.

- Relación entre las medidas de ciberseguridad y demás medidas de seguridad implementadas por las entidades críticas.

3) Determinación del proceso de designación o determinación de las entidades esenciales/ importantes.

- Especificar cuáles van a ser los requisitos para que las entidades de los tipos mencionados en los anexos I o II deban considerarse entidades esenciales.
- Especificar qué entidades de uno de los tipos mencionados en los anexos I o II vayan a ser catalogadas de importantes.
- Determinar qué empresas van a estar obligadas a presentar la información del art.3.4 para que los Estados miembros puedan elaborar sus listas.
- Establecer los mecanismos para que las entidades se puedan registrar como tales por sí mismas.

4) Diferenciación en el régimen de obligaciones de las entidades importantes y esenciales.

- NIS establece prácticamente las mismas obligaciones para unas y otras.
- Se debe establecer las diferencias del marco de obligaciones y supervisión de cada una de ellas.
- Se deben establecer las medidas de supervisión y ejecución que la autoridad competente debe poder adoptar con respecto a una u otra entidad.

5) Definición del marco de gobernanza pública, coordinación y asignación de competencias entre las autoridades responsables.

- Establecimiento de normas que regulen los mecanismos de intercambio de información sobre ciberseguridad entre autoridades competentes.

6) Definición concreta del marco de gobernanza interna para las empresas privadas que resulten obligadas.

- Definir las salvaguardas organizativas, normativas, procedimentales y tecnológicas necesarias para justificar un cumplimiento debido de la normativa.

- Incluir una definición básica de las funciones tecnológicas, organizativas y jurídicas que afectan a la ciberseguridad dentro de la compañía.

- Prever la periodicidad con la que miembros de los órganos de dirección y los empleados de las entidades esenciales e importantes deben asistir a formaciones específicas en materia de ciberseguridad. Así como elaborar un esquema sobre qué se entiende por formación específica y una aproximación a los contenidos mínimos.

- Determinar si se exige a las entidades esenciales o importantes que adquieran productos y servicios TIC certificados, de acuerdo con el art. 24.1.

- Establecer las consecuencias legales que puede asumir la persona física responsable de una entidad esencial por la vulneración de las obligaciones de NIS 2

7) Descripción de las medidas para la gestión de riesgos de ciberseguridad obligatorias.

- Determinar las medidas mínimas de gestión de riesgos de ciberseguridad para que las entidades excluidas del ámbito de aplicación de NIS 2 alcancen un elevado nivel de ciberseguridad (según establece el art.7.2.i).

8) Encaje de la figura del Responsable de Seguridad de la Información.

- Revisar sus funciones y responsabilidades conforme al nuevo esquema y en consonancia con el RD 43/2021.

9) Revisión del marco de notificación de incidentes.

- Velar por la coherencia con los marcos nacionales generales de gestión de crisis vigentes.

- Simplificar los trámites estableciendo un único punto de entrada y coordinando las actuaciones de las autoridades responsables.

- Delimitar cuáles son los “Incidentes significativos” y los “cuasiincientes” con mayor precisión, especialmente éstos últimos.

- Concretar los plazos de notificación en horas.

- Velar porque las personas físicas o jurídicas que así lo soliciten puedan notificar de forma anónima una vulnerabilidad al CSIRT designado.

10) Regular la adopción y revisión periódica de la estrategia nacional de ciberseguridad en consonancia con la obligación genérica establecida por la Directiva.

11) Conexión con el ENS.

- Aclarar el ámbito de aplicación del ENS en relación con las empresas privadas que son contratistas de la Administración Pública.

12) Establecimiento de un marco de regulación de las obligaciones de intercambio de información.

- Establecimiento de unas condiciones mínimas en consonancia con la directiva sobre los requisitos, condiciones y especificidades de los mecanismos tanto para las entidades públicas como privadas.

- Fomentar la puesta en común de ciberamenazas significativas y la cooperación efectiva, eficiente y segura con los CSIRT, las autoridades competentes o los puntos de contacto únicos.

13) Introducción de posibles mandatos legales de creación de estructuras de colaboración público-privada en materia de talento.

- Articulación de los fundamentos y principios que deben presidir la colaboración público-privada en la generación y la formación de capacidades diversas en materia de ciberseguridad (tecnológicas, legales, de comunicación, etc).

14) Definición y articulación de un régimen sancionador.

- Establecer el régimen de infracciones y las sanciones aplicables a cualquier incumplimiento.

- Regular la responsabilidad y las posibles infracciones que cometan los órganos de dirección de las entidades obligadas.

- Determinar si se podrán imponer multas coercitivas para obligar a una entidad esencial o importante a cesar en el incumplimiento de NIS 2.

15) Previsión de normas de rango reglamentario necesarias para desarrollar la ley.

- Normas de rango reglamentario que regule los requisitos, certificaciones y marco de gobernanza interna de las empresas obligadas. Así como la especificación del procedimiento sancionador.

- Definición de los contenidos mínimos obligatorios que debería incluir la formación en las compañías en materia de ciberseguridad.