ECIJA
Torre de Cristal Pº de la Castellana, 259C
28046 Madrid · Tel: +34 917 816 160
www.ecija.com

Nota informativa: Novedades Directiva NIS 2

Madrid, 9 de diciembre 2022

El pasado 28 de noviembre, Bruselas aprobó oficialmente la nueva Directiva de ciberseguridad, sobre seguridad de las redes y sistemas de información, derivado de las siglas en inglés *Network and Information Security,* también denominada NIS 2. Esta Directiva implica la sustitución de la actual Directiva sobre seguridad de las redes y sistemas de información, la conocida NIS, y forma parte de un paquete de normas europeas enfocadas en materia de ciberseguridad, entre las que destacan el reciente Reglamento aprobado sobre la resiliencia operativa digital para el sector financiero (el Reglamento DORA) y la Directiva sobre la resiliencia de las entidades críticas (CER).

En este sentido, la nueva Directiva NIS 2 tiene por objeto definir las bases para las medidas de gestión de riesgos de ciberseguridad de carácter consolidado en los distintos Estados Miembros, es decir, la armonización entre los Estados miembros con respecto a la prevención, detección, y respuesta ante incidentes de seguridad (especialmente ciberataques dirigidos tanto a sector público, como a sector privado cuando prestan servicios esenciales o importantes a la sociedad).

Esta actualización es consecuencia de la digitalización, a la que cada vez se suman más sectores y servicios interconectados. Esta interconexión, con beneficios indiscutibles, deriva también en que el número de amenazas ante las que se enfrentan tanto la sociedad, como los sectores público y privado, aumentan exponencialmente, siendo un asunto de especial preocupación en la Unión Europea, que con esta actualización normativa persigue reforzar los requisitos de seguridad y la coordinación de respuesta ante este tipo de incidentes.

Cabe resaltar que entre las novedades de NIS 2 para reforzar dichos aspectos, destaca la regulación de medidas de supervisión más robustas, así como nuevas obligaciones para los sujetos obligados.:

- Realización de análisis de riesgos sobre la seguridad de los sistemas de información
- Gestión de incidentes, continuidad negocio y gestión de crisis
- Seguridad de la cadena de suministro
- Implementación de políticas y procedimientos relativos a criptografía y cifrado
- Evaluación periódica de la eficacia de las medidas de seguridad implementadas
- Obligaciones reforzadas de notificación y colaboración sobre incidentes y vulnerabilidades

Con respecto a los sujetos obligados, además de los sectores que ya recogía la anterior Directiva NIS, es decir, sector sanitario, infraestructuras digitales, transporte, suministro de agua, energía, entidades financieras y proveedores de servicios digitales, NIS 2 amplía su ámbito de aplicación a nuevos sectores que considera "esenciales" o "importantes" para la sociedad:

- Proveedores de redes o servicios públicos de comunicaciones electrónica
- Gestión de aguas y residuos
- Fabricación de productos:
    - Productos informáticos, electrónicos y ópticos.
    - Material eléctrico.
    - Vehículos y material de transporte.

- Alimentación, incluyendo la producción, transformación y distribución de alimentos
- Sector sanitario: Se amplía a laboratorios de referencia, así como a entidades que fabrican productos farmacéuticos o productos sanitarios que son considerados esenciales, así como a entidades que realizan actividades de investigación clínica
- Sector aeroespacia
- Servicios digitales, ampliando a plataformas de servicios de redes sociales y centros de proceso de dato
- Servicios postales y de mensajería
- Administración pública

Tanto las administraciones públicas como toda entidad considerada mediana o gran empresa de los sectores indicados tendrán que cumplir con NIS2, pero además la propia Directiva establece situaciones donde se podrá aplicar a pequeñas empresas o microempresas: cuando dicha entidad sean único proveedor de un servicio en un Estado miembro, o la interrupción de su actividad pueda tener repercusiones sobre la seguridad pública, el orden público, o la salud pública.

Además, como novedad, la Directiva incluye por primera vez la ciberseguridad de la cadena de suministro de las TIC (aspecto que supone un cambio sustancial y relevante para los servicios vinculados con el Internet de las Cosas, conocido por sus siglas en inglés como IoT, *Internet of Things*).

Asimismo, merece especial atención la creación de una Red Europea de Organización de Enlace para Crisis Cibernéticas (EU-CyCLONe), que apoyará la gestión coordinada de incidentes y crisis de ciberseguridad a gran escala entre los distintos Estados miembro,

En cuanto a la notificación de incidentes de seguridad, la Directiva otorga un plazo de 24 horas desde que las entidades afectadas tienen conocimiento del incidente (que no tiene que por qué ser un incidente con efectos materiales, sino que basta con tener sospechas fundadas de su existencia), para presentar un informe inicial, debiendo presentar el informe final como máximo al mes de identificar el incidente.

Por último, y no menos importante, la Directiva prevé recursos y sanciones para garantizar su cumplimiento, determinando expresamente que,

1) **las entidades esenciales** que incumplan los artículos 21 (**medidas de gestión de riesgos de ciberseguridad**) o 23 (**obligación de reportar incidentes**) podrán enfrentarse a multas administrativas de un máximo de al menos **10.000.000 de euros o de un máximo de al menos el 2 % del volumen de negocios total anual a nivel mundial** en el ejercicio anterior de la empresa a la que pertenece la entidad esencial, lo que sea mayor.

2) **las entidades importantes**, que incumplan los artículos 21 (**medidas de gestión de riesgos de ciberseguridad**) o 23 (**obligación de reportar incidentes**) podrán enfrentarse a multas administrativas de un máximo de al menos **7 000 000 de euros o de un máximo de al menos el 1,4 % del volumen de negocios total anual a nivel mundial** en el ejercicio de la empresa a la que pertenezca la entidad importante, el que sea mayor.

Si bien la Directiva aún no ha sido publicada en el Diario Oficial de la Unión Europea, lo será en los próximos días. Desde el vigésimo día siguiente al de su publicación, los Estados miembros dispondrán de 21 meses para transponer la Directiva a legislación nacional.

Se esperan pocos cambios en dicha transposición, aunque sí lógicamente cierta concreción en las obligaciones, por lo que es importante que los nuevos sujetos obligados comiencen la implementación de sistemas de gestión de seguridad de la información que les permita el cumplimiento de las obligaciones indicadas llegado el momento.

Quedamos a su disposición para cualquier duda o cuestión que pudiera surgir.

Reciba un cordial un saludo,

Área de Ciberseguridad de ECIJA

info@ecija.com

Telf: + 34 91.781.61.60