AUGUSTAABOGADOS

ALERTA INFORMATIVA

19 de febrero de 2025

La Directiva NIS2 y el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad

La Directiva 2022/2555 también llamada Directiva NIS2 (Network and Information Security) es una normativa europea diseñada para mejorar la ciberseguridad en los Estados miembros de la Unión Europea definiendo obligaciones de ciberseguridad.
El anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad aprobado este pasado mes de enero es la normativa española en la que se va a trasponer la Directiva NIS2 y está en fase de tramitación urgente para que pueda ser aprobada a la mayor brevedad.

Objetivo Principal

La Directiva NIS2 busca garantizar un alto nivel común de ciberseguridad obligando a las empresas a implementar medidas de seguridad para la correcta gestión de riesgos y así proteger las redes y sistemas de información de sectores críticos y esenciales.

Ámbito de Aplicación

A diferencia de la anterior normativa, la NIS2 amplía el ámbito de aplicación incluyendo más sectores que deberán cumplir con sus obligaciones. Así, quedarán sujetas las entidades públicas y privadas descritas en el Anexo I y Anexo II de la Directiva, descritas como sectores de alta criticidad y sectores críticos independientemente del tamaño de la empresa o la organización.

Barcelona
Vía Augusta, 252, 4.ª
08017 Barcelona
T +34 933 621 620 ▫ **F** +34 932 009 843

Madrid
Antonio Maura, 18, 2.ª
28014 Madrid
T +34 911 592 323 ▫ **F** +34 911 592 322

Brussels (with IUROPE)
Avenue de Cortenbergh, 52
1000 Brussels (Belgium)
T +32 2 808 69 41

augustaabogados.com

Entre los sectores considerados de alta criticidad se encuentran: energía, transporte, banca, infraestructuras de los mercados financieros, sector sanitario, agua potable, aguas residuales, infraestructura digital.

Entre los sectores considerados críticos se encuentran las empresas y entidades públicas de los sectores: Servicios postales y de mensajería, gestión de residuos, fabricación, producción y distribución de sustancias y mezclas químicas, producción, transformación y distribución de alimentos, fabricación de productos sanitarios, informáticos, electrónicos, ópticos, material eléctrico, maquinara y equipo n.c.o.p, vehículos a motor, remolques y semirremolques, material de transporte y proveedores de servicios digitales.

Quedan excluidos del ámbito de aplicación defensa y seguridad nacional, seguridad pública, policía, el poder judicial o parlamentos y bancos centrales.

El anteproyecto establece dentro de su ámbito de aplicación las entidades públicas o privadas que tengan su residencia fiscal en España o, que, teniendo su residencia en otro Estado de la Unión Europea, ofrezcan sus servicios o desarrollen su actividad en nuestro país.

Creación del Centro Nacional de Ciberseguridad

El anteproyecto crea el Centro Nacional de Ciberseguridad como órgano encargado de dirigir, impulsar y coordinar dentro del ámbito de aplicación de esta normativa y se encargará también de hacer de órgano de contacto con la Unión Europea.

Obligaciones para las Empresas

Las empresas que entren dentro del ámbito de aplicación de la Directiva NIS2 deben implementar una serie de medidas de ciberseguridad que incluyen:

- **Gestión de riesgos**: análisis de riesgos y gestión de los mismos.
- **Aplicación de medidas de seguridad**: Protección de redes y sistemas y definición de políticas de seguridad.
- **Gestión de incidentes**: Procedimientos para detectar, gestionar y notificar incidentes de seguridad.
- **Continuidad del negocio**: Planificación y aplicación de medidas para garantizar la continuidad de los servicios.

Sanciones

La Directiva NIS2 establece unas sanciones en función del tipo de infracción y de la gravedad de sus consecuencias. Las cuantías económicas impuestas en el caso de sanción pueden oscilar de los 7 a 10 millones de euros o del 1,4% del volumen de negocio anual al 2%.

Impacto Comercial

Las empresas sujetas a las obligaciones de la Directiva NIS2 deben cumplirla por estar dentro del ámbito de aplicación, pero, además, poder demostrar el cumplimiento de esta normativa con la aplicación de medidas de seguridad adecuadas aumenta la confianza en los clientes y permite a las empresas destacar entre sus competidores.

Hoy en día, demostrar proactividad en el cumplimiento de las normativas de ciberseguridad trasmite a clientes, proveedores y socios tranquilidad y seguridad ante los riesgos de sufrir ciberataques y esto es siempre favorable para la reputación de la empresa.

Júlia Bacaria Gea. Socia
Departamento TMT | Augusta Abogados
j.bacaria@augustaabogados.com