DIRECTIVA NIS 2: AMBITO DE APLICACIÓN Y OBLIGACIONES PRINCIPALES

I. INTRODUCCIÓN

La Directiva 2022/2555, conocida como la NIS2, sustituye a la Directiva 2016/1148 (NIS1) y define obligaciones de ciberseguridad para los estados miembros con el objetivo de asegurar un alto nivel de protección en esta materia.

Esto incluye la implementación de medidas para gestionar riesgos de ciberseguridad, obligaciones de notificación para las entidades que se encuentran dentro de su alcance, así como responsabilidades en el intercambio de información sobre ciberseguirdad, así como obligaciones de supervisión y ejecución para los Estados.

El plazo para que los estados miembros adaptaran la Directiva NIS2 a sus legislaciones nacionales culminó el pasado 17 de octubre de 2024. Aunque la NIS2 entró en vigor el 16 de enero de 2023, su incorporación en España, al igual que en otros estados miembros, se ha retrasado debido a las complejidades legislativas y a la necesidad de adaptar las estructuras y normativas existentes.

El pasado enero, se ha publicado el anteproyecto de ley, que supondrá la trasposición al ordenamiento jurídico español de la Directiva, cuyo objetivo es fortalecer el marco comunitario de ciberseguridad al establecer requisitos para la protección de redes y sistemas de información.

II. ÁMBITO DE APLICACIÓN

La Directiva NIS2 amplía el número de sectores que se ven afectados por esta normativa. Su ámbito de aplicación se encuentra comprendido por entidades públicas o 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.

ANEXO I SECTORES DE ALTA CRITICIDAD
1. Energía: • Electricidad • Sistemas urbanos de calefacción y de refrigeración • Crudo • Gas • Hidrógeno 2. Transporte: • Aéreo • Ferrocarril • Marítimo y fluvial • Carretera 3. Banca 4. Infraestructuras de los mercados financieros 5. Sector sanitario 6. Agua potable 7. Aguas residuales 8. Infraestructura digital 9. Gestión de servicios TIC (de empresa a empresa) 10. Entidades de la Administración pública, con exclusión del poder judicial, los parlamentos y los bancos centrales. 11. Espacio

OTROS SECTORES CRÍTICOS
1. Servicios postales y de mensajería 2. Gestión de residuos 3. Fabricación, producción y distribución de sustancias y mezclas químicas 4. Producción, transformación y distribución de alimentos 5. Fabricación • Fabricación de productos sanitarios y productos sanitarios para diagnostico in vitro • Fabricación de productos informáticos, electrónicos y ópticos. • Fabricación de material eléctrico • Fabricación de maquinaria y equipo n.c.o.p • Fabricación de vehículos de motor, remolques y semirremolques • Fabricación de otro material de transporte 6. 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.

III. OBLIGACIONES

Las obligaciones para las empresas que se encuentren en su ámbito de aplicación es aplicar medidas para la gestión de riesgos de ciberseguridad. Estas medidas se resumen en los siguientes puntos:

a) Las políticas de seguridad de los sistemas de información y análisis de riesgos
b) La gestión de incidentes
c) La continuidad de las actividades, como la gestión de copias de seguridad y la recuperación en caso de catástrofe, y la gestión de crisis.
d) La seguridad de la cadena de suministro, incluidos los aspectos de seguridad relativos a las relaciones entre cada entidad y sus proveedores o prestadores de servicios directos;
e) La seguridad en la adquisición, el desarrollo y el mantenimiento de sistemas de redes y de información, incluida la gestión y la divulgación de las vulnerabilidades
f) Las políticas y los procedimientos para evaluar la eficacia de las medidas para la gestión de riesgos de ciberseguridad
g) Las prácticas básicas de ciberhigiene y formación en ciberseguridad
h) Las políticas y procedimientos relativos a la utilización de criptografía y, en su caso, de cifrado.
i) La seguridad de los recursos humanos, las políticas de control de acceso y la gestión de activos.
j) El uso de soluciones de autenticación multifactorial o de autenticación continua, comunicaciones de voz, vídeo y texto seguras y sistemas seguros de comunicaciones de emergencia en la entidad, cuando proceda.

IV. SANCIONES

Las sanciones pueden variar en cuantía en función de la gravedad de la infracción. Pero pueden llegar a 10 millones de euros o un máximo de un 2 % de volumen de negocio anual o a 7 millones de euros o a un máximo de un 1,4% del volumen de negocio anual.

Para más información sobre la aplicación de la NIS2 puede contactarnos.