Directiva NIS2: Aspectos claves

La Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, estableció medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión. LA Directiva es también conocida como Directiva NIS2.

Ya informamos en el momento de su aprobación de los aspectos más relevantes de la misma.

No obstante, el tiempo transcurrido y la falta de trasposición de la Directiva al ordenamiento jurídico español, está planteando un gran número de consultas en relación a la implantación en las empresas que operan en España de las prescripciones previstas en la Directiva.

Por ello, desde Escura consideramos conveniente destacar los aspectos más relevantes de la Directiva:

- **¿Cuál es el objeto de la Directiva?**

En primer lugar, debe destacarse que la Directiva NIS2 pretende alcanzar **un umbral común de ciberseguridad en todo el territorio de la Unión Europea** y, de este modo, mejorar el funcionamiento del mercado interior.

- **¿A qué entidades aplica la Directiva?**

La Directiva NIS2 es de aplicación a todas aquellas entidades públicas o privadas que tengan la consideración **de mediana y grandes empresas**, es decir aquellas que ocupen a **50 o más personas** trabajadoras y que tengan un **volumen de negocios anual superior a los 10 millones de euros**.

Asimismo, la Directiva también vincula, independientemente de su tamaño, a aquellas entidades que se dediquen a uno de los siguientes sectores críticos: energía, transporte, banca, infraestructura de mercados financieros, sector sanitario, agua potable y aguas residuales, infraestructura digital, gestión de servicios de TIC, entidades de la administración pública (con algunas excepciones), espacio, servicios postales y de mensajería, gestión de residuos, fabricación, producción y

distribución de sustancias y mezclas químicas, producción, transformación y distribución de alimentos, fabricación (productos sanitarios, informáticos, material eléctrico, maquinaria, vehículos de motor u otros materiales de transporte), proveedores de servicios digitales e investigación.

- **¿Qué medidas deben aplicar las entidades obligadas?**

Las entidades obligadas deberán adoptar las medidas técnicas, operativas y de organización adecuadas y proporcionadas para gestionar los riesgos en materia de seguridad de los sistemas de redes y de información. Entre estas:

a) Análisis y gestión de riesgos
b) Políticas de seguridad de la información
c) Gestión de incidentes
d) Continuidad de negocio y planes de recuperación
e) Seguridad de la cadena de suministro
f) Uso de criptografía y control de accesos
g) Formación en ciberseguridad

- **Responsabilidad personal**

La **dirección de las empresas**, y en concreto sus órganos de administración, son los **obligados a la adopción de las medidas**, y en caso de incumplimiento su **responsabilidad es personal**, incluyendo incluso la inhabilitación temporal para el ejercicio de la dirección de empresas.

Las sanciones se prevén hasta 10 millones o el 2% del facturado de la sociedad.

- **¿Cuándo entran en vigor las obligaciones para las entidades a nivel español?**

En la actualidad, el Gobierno ha elaborado y aprobado el Anteproyecto de Ley de Coordinación y Gobernanza de Ciberseguridad. No obstante, dicho anteproyecto está pendiente de tramitación parlamentaria, por lo que el mismo todavía no ha sido aprobado, si bien el cumplimiento de la Directiva es de obligado cumplimiento para las empresas obligadas.