DIRECTIVA NIS 2: ÀMBIT D'APLICACIÓ I OBLIGACIONS PRINCIPALS

I. INTRODUCCIÓ

La Directiva 2022/2555, coneguda com la NIS2, substitueix a la Directiva 2016/1148 (NIS1) i defineix obligacions de ciberseguretat per als estats membres amb l'objectiu d'assegurar un alt nivell de protecció en aquesta matèria.

Això inclou la implementació de mesures per a gestionar riscos de ciberseguretat, obligacions de notificació per a les entitats que es troben dins del seu abast, així com responsabilitats en l'intercanvi d'informació sobre *ciberseguirdad, així com obligacions de supervisió i execució per als Estats.

El termini perquè els estats membres adaptessin la Directiva NIS2 a les seves legislacions nacionals va culminar el passat 17 d'octubre de 2024. Encara que la NIS2 va entrar en vigor el 16 de gener de 2023, la seva incorporació a Espanya, igual que en altres estats membres, s'ha retardat a causa de les complexitats legislatives i a la necessitat d'adaptar les estructures i normatives existents.

El gener passat, s'ha publicat l'avantprojecte de llei, que suposarà la trasposició a l'ordenament jurídic espanyol de la Directiva, l'objectiu de la qual és enfortir el marc comunitari de ciberseguretat en establir requisits per a la protecció de xarxes i sistemes d'informació.

II. ÀMBIT D'APLICACIÓ

La Directiva NIS2 amplia el nombre de sectors que es veuen afectats per aquesta normativa. El seu àmbit d'aplicació es troba comprès per entitats públiques o privades descrites en l'Annex I i Annex II de la Directiva, descrites com a sectors d'alta criticitat i sectors crítics independentment de la grandària de l'empresa.

ANNEX I SECTORS D'ALTA CRITICITAT
1. Energia: • Electricitat • Sistemes urbans de calefacció i de refrigeració • Cru • Gas • Hidrogen 2. Transport: • Aeri • Ferrocarril • Marítim i fluvial • Carretera 3. Banca 4. Infraestructures dels mercats financers 5. Sector sanitari 6. Aigua potable 7. Aigües residuals 8. Infraestructura digital 9. Gestió de serveis TIC (d'empresa a empresa) 10. Entitats de l'Administració pública, a exclusió del poder judicial, els parlaments i els bancs centrals. 11. Espai

ALTRES SECTORS CRÍTICS
1. Serveis postals i de missatgeria 2. Gestió de residus 3. Fabricació, producció i distribució de substàncies i mescles químiques 4. Producció, transformació i distribució d'aliments 5. Fabricació • Fabricació de productes sanitaris i productes sanitaris per a diagnostico in vitro • Fabricació de productes informàtics, electrònics i òptics. • Fabricació de material elèctric • Fabricació de maquinària i equipo n.c.o.p • Fabricació de vehicles de motor, remolcs i semiremolcs • Fabricació d'un altre material de transport 6. Proveïdors de serveis digitals

Queden exclosos de l'àmbit d'aplicació defensa i seguretat nacional, seguretat pública, policia, el poder judicial o parlaments i bancs centrals.

III. OBLIGACIONS

Les obligacions per a les empreses que es trobin en el seu àmbit d'aplicació és aplicar mesures per a la gestió de riscos de ciberseguretat. Aquestes mesures es resumeixen en els següents punts:

a) Les polítiques de seguretat dels sistemes d'informació i anàlisi de riscos
b) La gestió d'incidents
c) La continuïtat de les activitats, com la gestió de còpies de seguretat i la recuperació en cas de catàstrofe, i la gestió de crisi.
d) La seguretat de la cadena de subministrament, inclosos els aspectes de seguretat relatius a les relacions entre cada entitat i els seus proveïdors o prestadors de serveis directes;
e) La seguretat en l'adquisició, el desenvolupament i el manteniment de sistemes de xarxes i d'informació, inclosa la gestió i la divulgació de les vulnerabilitats
f) Les polítiques i els procediments per a avaluar l'eficàcia de les mesures per a la gestió de riscos de ciberseguretat
g) Les pràctiques bàsiques de *ciberhigiene i formació en ciberseguretat
h) Les polítiques i procediments relatius a la utilització de criptografia i, si és el cas, de xifratge.
i) La seguretat dels recursos humans, les polítiques de control d'accés i la gestió d'actius.
j) L'ús de solucions d'autenticació multifactorial o d'autenticació contínua, comunicacions de veu, vídeo i text segures i sistemes segurs de comunicacions d'emergència en l'entitat, quan escaigui.

IV. SANCIONS

Les sancions poden variar en quantia en funció de la gravetat de la infracció. Però poden arribar a 10 milions d'euros o un màxim d'un 2% de volum de negoci anual o a 7 milions d'euros o a un màxim d'un 1,4% del volum de negoci anual.

Per a més informació sobre l'aplicació de la NIS2 pot contactar-nos.