LES PÍNDOLES DEL DPD

PÍNDOLA 67.- ENTRA EN VIGOR LA DIRECTIVA NIS2, LA LEGISLACIÓ EN MATÈRIA DE CIBERSEGURETAT ADOPTADA PER A TOTA LA UNIÓ EUROPEA

I. INTRODUCCIÓ

La Directiva 2022/2555, coneguda com a NIS2, substitueix a la Directiva 2016/1148 (NIS1) i estableix obligacions de ciberseguretat per als estats membres per tal de garantir un alt nivell de ciberseguretat, a través de mesures per a la **gestió de riscos de ciberseguretat**, obligacions de **notificació** per a les entitats en el seu àmbit d'aplicació i obligacions relatives a **l'intercanvi d'informació sobre ciberseguretat**, així com obligacions de **supervisió i execució** per als estats.

El passat dijous **17 d'octubre de 2024** va finalitzar el termini perquè els estats membres transposessin a les seves legislacions nacionals la Directiva NIS2. Tot i que la **NIS2 va entrar en vigor el 16 de gener de 2023**, la seva transposició a Espanya, com en altres estats membres, s'ha endarrerit a causa de complexitats legislatives i la necessitat d'adaptar les estructures i normatives actuals. **L'evidència de transposició es farà a través del BOE**, que, com és preceptiu, **publicarà la norma de transposició**, assenyalant per a ella la data en la qual entri en vigor i, eventualment, la **data en la qual serà de plena aplicació**, que podrà ser més tard.

II. ÀMBIT D'APLICACIÓ

La NIS2 amplia l'abast de la directiva original, que cobria principalment operadors de serveis essencials. Amb la nova directiva, sectors addicionals, com proveïdors de serveis digitals i diverses indústries estratègiques com els **sectors de l'energia, transport, aigua, infraestructura digital, gestió dels serveis TIC, entitats de l'administració pública**, que hauran de complir amb requisits de ciberseguretat més exigents, cosa que incrementa la pressió en el procés d'adequació legislativa.

També s'aplicarà al **sector sanitari**, concretament les **entitats que prestin serveis d'assistència sanitària** (Art.3, lletra g) de la Directiva 2011/24/UE), **laboratoris de referència de la UE** (tal com es defineixen en l'Art.15 del Reglament UE 2022/2371), **entitats que duguin a terme activitats d'investigació i desenvolupament de medicaments** (Art. 1 de la Directiva 2001/83/CE), **entitats que fabriquin productes farmacèutics de base i especialitats farmacèutiques** (Secció C de la NACE Rev. 2) i **entitats que fabriquin productes sanitaris que es consideren essencials en situacions d'emergència de salut pública** (Art.22 del Reglament UE 2022/123).

III. PRINCIPALS NOVETATS

Les principals novetats de la directiva NIS2, respecte a la seva antecessora, són les següents:

- **L'ampliació de sectors** als quals haurà d'aplicar-se: energia, transport, banca, sanitat, aigua potable, administració pública, serveis postals, gestió residus indústria química, etc.
- Promoure la **cooperació entre entitats del sector públic i privat** per al desenvolupament d'estratègies nacionals dels diferents estats membres.
- **Harmonitzar** la normativa que regula la **prevenció, detecció i resposta a ciberatacs**.
- L'Agència de la Unió Europea per a la Ciberseguretat (**ENISA**) serà responsable de la seva promoció, entre els estats membres.
- S'estableixen nous requisits de seguretat com la resposta davant incidents, la **seguretat de la cadena de subministrament**, el xifratge i la divulgació de vulnerabilitats.
- La ciberseguretat passarà a ser **responsabilitat dels alts càrrecs** directius de l'entitat.
- Els **estats membres establiran el règim sancionador**, aplicable a les infraccions adoptades en la Directiva, sent les sancions efectives, proporcionades i dissuasives.

En relació amb les **obligacions dels estats membres**, la nova directiva els exigeix mantenir i comunicar un **llistat d'entitats essencials**, a més d'elaborar una **estratègia nacional de ciberseguretat**. Han de designar autoritats competents, equips de resposta a incidents (**CSIRT**) i establir un pla nacional per gestionar les crisis de ciberseguretat. També es fomenta la **cooperació i l'intercanvi d'informació** en l'àmbit nacional i europeu per a una resposta efectiva a les amenaces cibernètiques. Finalment, s'exigeix supervisió, mesures de gestió de riscos, notificació d'incidents i formació dels gestors en ciberseguretat.

IV. MESURES DE SEGURETAT

Les entitats incloses en l'abast de la NIS2 hauran de complir una sèrie de mesures tècniques, operatives i d'organització per a una adequada gestió de riscos de ciberseguretat. En el cas que l'entitat disposi de certificat amb **l'Esquema Nacional de Seguretat** (RD 311/2022) en nivell:

- **ALT:** Complirà amb les mesures indicades en la NIS2

- **MITJÀ / BAIX:** S'hauran d'implementar aquelles mesures derivades de l'anàlisi dels riscos inherents a cada entitat per a verificar quines mesures cal adoptar i amb quins reforços.

- **En cas de no estar certificat amb l'ENS:** S'hauran d'implementar aquelles mesures tècniques, operatives i organitzatives adequades i proporcionades per a la gestió de riscos i incloure almenys els elements indicats a l'Article 21 de la NIS2:

LES PÍNDOLES DEL DPD

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 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

Sobre la base dels treballs desenvolupats pel Grup de Cooperació NIS2 de la UE, i a les mesures recomanades o suggerides per aquest grup de treball, el ***Centro Criptológico Nacional*** (CCN), sense perjudici del resultat final de la transposició de la NIS2 a Espanya i de les eventuals adaptacions que haguessin d'incorporar-se, ha publicat la guia CCN-STIC 892, un **perfil de compliment específic per a organitzacions en l'àmbit d'aplicació de la Directiva NIS2**. L'objectiu d'aquest document és oferir un perfil per donar resposta a les disposicions de la directiva europea per a les organitzacions que es troben dins l'àmbit de l'Esquema Nacional de Seguretat (ENS).

Podeu consultar la directiva sencera així com material relacionat als següents enllaços:

https://www.boe.es/doue/2022/333/L00080-00152.pdf
https://www.ccn.cni.es/es/normativa/directiva-nis2
https://www.ccn-cert.cni.es/es/seguridad-al-dia/novedades-ccn-cert/12945-el-ccn-publica-un-nuevo-perfil-de-cumplimiento-especifico-para-organizaciones-en-el-ambito-de-aplicacion-de-la-directiva-nis2.html

Per qualsevol dubte o aclariment addicional, us podeu adreçar al DPD de Salut:

dpd@ticsalutsocial.cat
https://ticsalutsocial.cat/oficina-dpd/
Tel.: 93 553 26 42 (9:00 a 14:00 h)