



RECURS GRATUÏT · AUTOAVALUACIÓ

Checklist de Compliment NIS2

47 comprovacions per diagnosticar la teva preparació NIS2 en uns deu minuts. Cadascuna indica l'article d'on surt, perquè puguis comprovar tu mateix la font.

Angel Sulev · Chief Architect of Secure AI · ANSULEV Group

Estat normatiu revisat: **2026-10-07** · Versió 1.0

ansulev.com · info@ansulev.com

Com fer servir aquest checklist

Respon cada punt amb honestetat: **Sí** (implantat i amb evidències), **Parcial** (existeix, però sense documentar, sense provar o incomplet) o **No**. Si no pots mostrar l'evidència, la resposta és Parcial.

- Les referències remetent a la Directiva (UE) 2022/2555 (NIS2) llevat que s'indiqui una altra cosa.
- Els punts marcats **ES** provenen de l'avantprojecte espanyol de transposició i poden canviar abans de la seva aprovació.
- Al final calcula la teva puntuació. Les franges serveixen per prioritzar; no són una opinió jurídica.

Què hi ha en joc

- Multes per incomplir els arts. 21 o 23: màxim d'almenys **10 M€ o el 2 %** del volum de negoci mundial per a entitats essencials i **7 M€ o l'1,4 %** per a entitats importants, la xifra més alta (art. 34.4–5).
- Els òrgans de direcció aproven les mesures, en supervisen l'aplicació i **poden ser considerats responsables** (art. 20.1). En entitats essencials, el conseller delegat o representant legal pot ser inhabilitat temporalment per exercir funcions de direcció (art. 32.5.b).
- Terminis davant d'incidents: alerta primerenca en **24 h**, notificació en **72 h**, informe final en **un mes** (art. 23.4).

Espanya: situació a 2026-10-07

- La NIS2 **encara no està transposada** a Espanya. El Consell de Ministres va aprovar l'*Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad* el 14 de gener de 2025 i no s'ha publicat al BOE.
- El 8 de juliol de 2026 la Comissió Europea va portar Espanya, França, Irlanda i els Països Baixos davant del Tribunal de Justícia per no notificar la transposició completa.
- Mentre no entri en vigor la nova llei, continuen aplicant-se el **RD-ley 12/2018** i el **RD 43/2021** (NIS1). CSIRT de referència: INCIBE-CERT (sector privat) i CCN-CERT (sector públic).
- L'avantprojecte replica els terminis de 24 h / 72 h / un mes, crea un *Centro Nacional de Ciberseguridad* i pren l'ENS (RD 311/2022) com a base de les mesures de seguretat.

Les obligacions europees ja estan fixades i muntar un programa amb evidències porta mesos: esperar el BOE et costa aquest temps.

1 • Àmbit i registre

#	COMPROVACIÓ	REFERÈNCIA	ESTAT
01	Has creuat cada servei que prestes amb els sectors i subsectors de l' annex I (alta criticitat) i de l' annex II (altres sectors crítics).	Art. 2.1, annexos I-II	☐ S ☐ P ☐ N
02	Has comprovat si la teva organització és mitjana empresa o més gran : 50 o més treballadors, o volum de negoci i balanç tots dos superiors a 10 M€, comptant empreses associades i vinculades.	Art. 2.1; Rec. 2003/361/CE	☐ S ☐ P ☐ N
03	Has revisat els supòsits que s'apliquen sigui quina sigui la mida : telecomunicacions, serveis de confiança, TLD/DNS, registre de dominis, proveïdor únic nacional d'un servei essencial, entitat crítica, Administració pública.	Art. 2.2-2.4	☐ S ☐ P ☐ N
04	Saps si ets entitat essencial o important i el raonament està documentat.	Art. 3.1-3.2	☐ S ☐ P ☐ N
05	Has identificat la normativa sectorial de la UE amb requisits equivalents que pugui prevaler (per exemple DORA en entitats financeres).	Art. 4	☐ S ☐ P ☐ N
06	Les dades de registre estan preparades: nom, adreça, contacte amb correu, telèfon i rangs IP , sector i estats membres on operes. Els canvis es comuniquen en dues setmanes.	Art. 3.4; art. 27 (proveïdors digitals)	☐ S ☐ P ☐ N
07	Has designat un Responsable de la Seguretat de la Informació (persona, unitat o òrgan col·legiat, amb substitut) com a punt de contacte amb l'autoritat de control i el CSIRT. ES	Avantprojecte art. 16	☐ S ☐ P ☐ N
08	Saps si t'és aplicable l' ENS (RD 311/2022). A l'avantprojecte, el perfil de compliment específic de l'ENS acredita les mesures; les entitats essencials s'han de certificar i les importants es poden autoavaluar. ES	Avantprojecte art. 15.2, 15.4	☐ S ☐ P ☐ N

2 • Governança i responsabilitat de la direcció

#	COMPROVACIÓ	REFERÈNCIA	ESTAT
09	L'òrgan de direcció ha aprobat formalment les mesures de gestió de riscos de ciberseguretat, amb registre datat.	Art. 20.1	☐ S ☐ P ☐ N
10	L'òrgan de direcció supervisa la seva aplicació amb informes periòdics sobre estat, mancances i incidents.	Art. 20.1	☐ S ☐ P ☐ N
11	Els membres de l'òrgan de direcció han rebut formació en ciberseguretat i l'assistència en consta.	Art. 20.2	☐ S ☐ P ☐ N
12	S'ofereix formació similar als treballadors de manera periòdica .	Art. 20.2	☐ S ☐ P ☐ N
13	La direcció entén la seva responsabilitat personal , inclosa la responsabilitat per infraccions i, en entitats essencials, la possible inhabilitació temporal per a funcions de direcció.	Art. 20.1, 32.5.b, 32.6	☐ S ☐ P ☐ N
14	Hi ha un responsable del compliment NIS2 amb nom, recursos suficients i comunicació directa amb el consell.	Art. 20.1; avantprojecte art. 16.4	☐ S ☐ P ☐ N

3 • Mesures de gestió de riscos (article 21)

Les deu mesures mínimes de l'art. 21.2, lletres a) a j), més proporcionalitat i cadena de subministrament.

#	COMPROVACIÓ	REFERÈNCIA	ESTAT
15	Hi ha una política de seguretat dels sistemes d'informació documentada, aprovada i revisada periòdicament.	Art. 21.2.a	☐ S ☐ P ☐ N
16	Mantens una anàlisi de riscos amb un enfocament de tots els perills, inclòs l'entorn físic dels sistemes.	Art. 21.1–21.2.a	☐ S ☐ P ☐ N
17	Un procediment de gestió d'incidents cobreix detecció, triatge, contenció, recuperació i lliçons apreses.	Art. 21.2.b	☐ S ☐ P ☐ N
18	El registre d'esdeveniments i la monitorització permeten detectar un incident i reconstruir què ha passat.	Art. 21.2.b	☐ S ☐ P ☐ N
19	Les còpies de seguretat estan definides, protegides contra manipulacions i les restauracions es proven .	Art. 21.2.c	☐ S ☐ P ☐ N
20	Hi ha un pla de recuperació davant desastres amb objectius de recuperació i s'ha assajat.	Art. 21.2.c	☐ S ☐ P ☐ N
21	La gestió de crisi està definida: rols, capacitat de decisió i comunicació per un canal alternatiu.	Art. 21.2.c	☐ S ☐ P ☐ N
22	Mantens un inventari de proveïdors directes i prestadors de serveis, classificats per criticitat.	Art. 21.2.d	☐ S ☐ P ☐ N
23	Avalues els proveïdors crítics per les seves vulnerabilitats, la qualitat dels seus productes i el seu desenvolupament segur .	Art. 21.3	☐ S ☐ P ☐ N
24	Els contractes amb proveïdors inclouen requisits de seguretat, obligació de notificar incidents i dret d'auditoria.	Art. 21.2.d	☐ S ☐ P ☐ N
25	Tens en compte les avaluacions coordinades de riscos de la UE sobre cadenes de subministrament crítiques (per exemple 5G).	Art. 21.3, 22.1	☐ S ☐ P ☐ N
26	La seguretat forma part de l' adquisició, el desenvolupament i el manteniment : desenvolupament segur i gestió de canvis.	Art. 21.2.e	☐ S ☐ P ☐ N
27	La gestió de vulnerabilitats és contínua: escaneig, aplicació de pegats prioritzada i terminis amb seguiment.	Art. 21.2.e	☐ S ☐ P ☐ N
28	Un canal públic de divulgació de vulnerabilitats permet que tercers et comuniquin errors.	Art. 21.2.e; art. 12	☐ S ☐ P ☐ N
29	Avalues l' eficàcia de les mesures de manera planificada: auditories, proves i mètriques.	Art. 21.2.f	☐ S ☐ P ☐ N
30	Cada incompliment detectat activa mesures correctores sense demora indeguda i se'n fa el seguiment fins al tancament.	Art. 21.4	☐ S ☐ P ☐ N
31	Appliques una línia base de ciberhigiene : bastionatge, configuració segura, pegats i mínima funcionalitat.	Art. 21.2.g	☐ S ☐ P ☐ N
32	Tota la plantilla rep formació de conscienciació , inclosa la de phishing.	Art. 21.2.g	☐ S ☐ P ☐ N
33	Una política de criptografia defineix algorismes aprovats i el cicle de vida de les claus.	Art. 21.2.h	☐ S ☐ P ☐ N

34	Les dades es xifren en trànsit i en repòs quan escau.	Art. 21.2.h	☐ S ☐ P ☐ N
35	La seguretat dels recursos humans cobreix altes, canvis i baixes, confidencialitat i verificacions lícites.	Art. 21.2.i	☐ S ☐ P ☐ N
36	El control d'accés segueix el mínim privilegi, els accessos privilegiats estan gestionats i els permisos es revisen periòdicament.	Art. 21.2.i	☐ S ☐ P ☐ N
37	Mantens al dia un inventari d'actius : maquinari, programari, dades i responsables.	Art. 21.2.i	☐ S ☐ P ☐ N
38	L' autenticació multifactor o contínua protegeix l'accés remot, administratiu i crític.	Art. 21.2.j	☐ S ☐ P ☐ N
39	Quan escau, hi ha comunicacions de veu, vídeo i text segures i un sistema segur de comunicacions d'emergència .	Art. 21.2.j	☐ S ☐ P ☐ N
40	Has documentat per què les teves mesures són proporcionades a la teva exposició, la mida, i la probabilitat i gravetat dels incidents.	Art. 21.1	☐ S ☐ P ☐ N
41	Si ets proveïdor de DNS, TLD, núvol, centre de dades, CDN, serveis gestionats (MSP/MSSP), mercat en línia, cercador, xarxa social o serveis de confiança, les teves mesures estan mapades al Reglament d'Execució (UE) 2024/2690 .	Art. 21.5; Regl. 2024/2690	☐ S ☐ P ☐ N

4 • Notificació d'incidents i supervisió

#	COMPROVACIÓ	REFERÈNCIA	ESTAT
42	Els teus criteris d' incident significatiu estan escrits: pertorbació operativa greu o pèrdues econòmiques, o danys considerables a tercers.	Art. 23.3; Regl. 2024/2690	☐ S ☐ P ☐ N
43	Un procediment d' alerta primerenca en 24 hores fixa qui decideix, qui l'envia, a quin CSIRT i com funciona fora d'horari.	Art. 23.4.a	☐ S ☐ P ☐ N
44	Pots emetre una notificació d'incident en 72 hores amb una avaluació inicial de gravetat, impacte i indicadors de compromís.	Art. 23.4.b	☐ S ☐ P ☐ N
45	Pots lliurar un informe final en un mes (causa arrel, mitigació, impacte transfronterer) o un informe de situació si l'incident continua obert.	Art. 23.4.d-e	☐ S ☐ P ☐ N
46	Saps com informar els destinataris dels teus serveis d'incidents i amenaces significatives. La notificació de violació de dades a l'AEPD pel RGPD (72 h) va en paral·lel.	Art. 23.1-23.2; RGPD art. 33	☐ S ☐ P ☐ N
47	Tens a punt un paquet d'evidències per al supervisor: polítiques documentades, resultats d'auditoria i proves d'implantació.	Art. 32.2.e-g, 33.2.d-f	☐ S ☐ P ☐ N

La teva puntuació

Compta **2 punts** per cada Sí, **1** per cada Parcial i **0** per cada No. Màxim: 94.

Punts	Lectura
80–94	Base sòlida. Centra't en la qualitat de les evidències i en la prova de la teva cadena de notificació de 24 h / 72 h.
50–79	Mancances reals. Prioritza governança (secció 2) i notificació (secció 4): solen ser el més ràpid de corregir.
0–49	Comença per l'àmbit, l'aprovació del consell i un procediment d'incidents. El pas següent és una anàlisi de mancances estructurada.

Aquestes franges són una ajuda orientativa per prioritzar, no una determinació de compliment.

Vols una altra mirada sobre les teves mancances?

Reserva una trucada i porta la teva puntuació. Revisarem les teves tres seccions més febles i què cal corregir primer.

calendly.com/ansulev · info@ansulev.com · ansulev.com/ca

Fonts

Directiva (UE) 2022/2555 (NIS2), DO L 333 de 27.12.2022 · Reglament d'Execució (UE) 2024/2690 de la Comissió · ENISA, *Technical Implementation Guidance on Cybersecurity Risk Management Measures*, v1.0, juny de 2025 · Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad (Ministerio del Interior, notificació TRIS 26686) · Comissió Europea, remissió al TJUE per la NIS2, 8 de juliol de 2026 · RD-ley 12/2018 i RD 43/2021.

Canvis europeus pendants, sense força de llei a 2026-10-07: el Digital Omnibus (punt únic de notificació d'incidents, proposat el 19 de novembre de 2025) i les modificacions de la NIS2 COM(2026) 13 (proposades el 20 de gener de 2026).

Aquest checklist és informació general, no assessorament jurídic. Les teves obligacions depenen del teu sector, la mida, l'estat membre i la llei nacional definitiva.

© Angel Georgiev Sulev · Tots els drets reservats