



RECURSO GRATUITO · AUTOEVALUACIÓN

Checklist de Cumplimiento NIS2

47 comprobaciones para diagnosticar tu preparación NIS2 en unos diez minutos. Cada una indica el artículo del que sale, para que puedas comprobar tú mismo la fuente.

Angel Sulev · Chief Architect of Secure AI · ANSULEV Group

Estado normativo revisado: **2026-10-07** · Versión 1.0

ansulev.com · info@ansulev.com

Cómo usar este checklist

Responde a cada punto con honestidad: **Sí** (implantado y con evidencias), **Parcial** (existe, pero sin documentar, sin probar o incompleto) o **No**. Si no puedes mostrar la evidencia, la respuesta es Parcial.

- Las referencias remiten a la Directiva (UE) 2022/2555 (NIS2) salvo que se indique otra cosa.
- Los puntos marcados **ES** proceden del anteproyecto español de transposición y pueden cambiar antes de su aprobación.
- Al final calcula tu puntuación. Las franjas sirven para priorizar; no son una opinión jurídica.

Qué está en juego

- Multas por incumplir los arts. 21 o 23: máximo de al menos **10 M€ o el 2 %** del volumen de negocios mundial para entidades esenciales y **7 M€ o el 1,4 %** para entidades importantes, la cifra mayor (art. 34.4–5).
- Los órganos de dirección aprueban las medidas, supervisan su aplicación y **pueden ser considerados responsables** (art. 20.1). En entidades esenciales cabe la prohibición temporal de ejercer funciones de dirección al consejero delegado o representante legal (art. 32.5.b).
- Plazos ante incidentes: alerta temprana en **24 h**, notificación en **72 h**, informe final en **un mes** (art. 23.4).

España: situación a 2026-10-07

- NIS2 **todavía no está transpuesta** en España. El Consejo de Ministros aprobó el *Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad* el 14 de enero de 2025 y no se ha publicado en el BOE.
- El 8 de julio de 2026 la Comisión Europea llevó a España, Francia, Irlanda y Países Bajos ante el Tribunal de Justicia por no notificar la transposición completa.
- Mientras no entre en vigor la nueva ley siguen aplicándose el **RD-ley 12/2018** y el **RD 43/2021** (NIS1). CSIRT de referencia: INCIBE-CERT (sector privado) y CCN-CERT (sector público).
- El anteproyecto replica los plazos de 24 h / 72 h / un mes, crea un *Centro Nacional de Ciberseguridad* y toma el ENS (RD 311/2022) como base de las medidas de seguridad.

Las obligaciones europeas ya están fijadas y montar un programa con evidencias lleva meses: esperar al BOE te cuesta ese tiempo.

1 • Ámbito y registro

#	COMPROBACIÓN	REFERENCIA	ESTADO
01	Has cruzado cada servicio que prestas con los sectores y subsectores del anexo I (alta criticidad) y del anexo II (otros sectores críticos).	Art. 2.1, anexos I-II	☐ S ☐ P ☐ N
02	Has comprobado si tu organización es mediana empresa o mayor : 50 o más empleados, o volumen de negocios y balance ambos superiores a 10 M€, contando empresas asociadas y vinculadas.	Art. 2.1; Rec. 2003/361/CE	☐ S ☐ P ☐ N
03	Has revisado los supuestos que aplican sin importar el tamaño : telecomunicaciones, servicios de confianza, TLD/DNS, registro de dominios, proveedor único nacional de un servicio esencial, entidad crítica, Administración pública.	Art. 2.2-2.4	☐ S ☐ P ☐ N
04	Sabes si eres entidad esencial o importante y el razonamiento está documentado.	Art. 3.1-3.2	☐ S ☐ P ☐ N
05	Has identificado la normativa sectorial de la UE con requisitos equivalentes que pueda prevalecer (por ejemplo DORA en entidades financieras).	Art. 4	☐ S ☐ P ☐ N
06	Los datos de registro están preparados: nombre, dirección, contacto con email, teléfono y rangos IP , sector y Estados miembros donde operas. Los cambios se comunican en dos semanas.	Art. 3.4; art. 27 (proveedores digitales)	☐ S ☐ P ☐ N
07	Has designado un Responsable de la Seguridad de la Información (persona, unidad u órgano colegiado, con sustituto) como punto de contacto con la autoridad de control y el CSIRT. ES	Anteproyecto art. 16	☐ S ☐ P ☐ N
08	Sabes si te aplica el ENS (RD 311/2022). En el anteproyecto, el perfil de cumplimiento específico del ENS acredita las medidas; las entidades esenciales deben certificarse y las importantes pueden autoevaluarse. ES	Anteproyecto art. 15.2, 15.4	☐ S ☐ P ☐ N

2 • Gobernanza y responsabilidad de la dirección

#	COMPROBACIÓN	REFERENCIA	ESTADO
09	El órgano de dirección ha aprobado formalmente las medidas para la gestión de riesgos de ciberseguridad, con registro fechado.	Art. 20.1	☐ S ☐ P ☐ N
10	El órgano de dirección supervisa su aplicación con informes periódicos sobre estado, carencias e incidentes.	Art. 20.1	☐ S ☐ P ☐ N
11	Los miembros del órgano de dirección han recibido formación en ciberseguridad y la asistencia consta.	Art. 20.2	☐ S ☐ P ☐ N
12	Se ofrece formación similar a los empleados de forma periódica .	Art. 20.2	☐ S ☐ P ☐ N
13	La dirección entiende su responsabilidad personal , incluida la responsabilidad por infracciones y, en entidades esenciales, la posible inhabilitación temporal para funciones de dirección.	Art. 20.1, 32.5.b, 32.6	☐ S ☐ P ☐ N
14	Hay un responsable del cumplimiento NIS2 con nombre, recursos suficientes y comunicación directa con el consejo.	Art. 20.1; anteproyecto art. 16.4	☐ S ☐ P ☐ N

3 • Medidas de gestión de riesgos (artículo 21)

Las diez medidas mínimas del art. 21.2, letras a) a j), más proporcionalidad y cadena de suministro.

#	COMPROBACIÓN	REFERENCIA	ESTADO
15	Existe una política de seguridad de los sistemas de información documentada, aprobada y revisada periódicamente.	Art. 21.2.a	☐ S ☐ P ☐ N
16	Mantienes un análisis de riesgos con enfoque de todos los peligros, incluido el entorno físico de los sistemas.	Art. 21.1–21.2.a	☐ S ☐ P ☐ N
17	Un procedimiento de gestión de incidentes cubre detección, triaje, contención, recuperación y lecciones aprendidas.	Art. 21.2.b	☐ S ☐ P ☐ N
18	El registro de eventos y la monitorización permiten detectar un incidente y reconstruir lo ocurrido.	Art. 21.2.b	☐ S ☐ P ☐ N
19	Las copias de seguridad están definidas, protegidas frente a manipulación y las restauraciones se prueban .	Art. 21.2.c	☐ S ☐ P ☐ N
20	Existe un plan de recuperación ante desastres con objetivos de recuperación y se ha ensayado.	Art. 21.2.c	☐ S ☐ P ☐ N
21	La gestión de crisis está definida: roles, capacidad de decisión y comunicación por canal alternativo.	Art. 21.2.c	☐ S ☐ P ☐ N
22	Mantienes un inventario de proveedores directos y prestadores de servicios, clasificados por criticidad.	Art. 21.2.d	☐ S ☐ P ☐ N
23	Evalúas a los proveedores críticos por sus vulnerabilidades, la calidad de sus productos y su desarrollo seguro .	Art. 21.3	☐ S ☐ P ☐ N
24	Los contratos con proveedores incluyen requisitos de seguridad, obligación de notificar incidentes y derecho de auditoría.	Art. 21.2.d	☐ S ☐ P ☐ N
25	Tienes en cuenta las evaluaciones coordinadas de riesgos de la UE sobre cadenas de suministro críticas (por ejemplo 5G).	Art. 21.3, 22.1	☐ S ☐ P ☐ N
26	La seguridad forma parte de la adquisición, el desarrollo y el mantenimiento : desarrollo seguro y gestión de cambios.	Art. 21.2.e	☐ S ☐ P ☐ N
27	La gestión de vulnerabilidades es continua: escaneo, parcheo priorizado y plazos con seguimiento.	Art. 21.2.e	☐ S ☐ P ☐ N
28	Un canal público de divulgación de vulnerabilidades permite que terceros te reporten fallos.	Art. 21.2.e; art. 12	☐ S ☐ P ☐ N
29	Evalúas la eficacia de las medidas de forma planificada: auditorías, pruebas y métricas.	Art. 21.2.f	☐ S ☐ P ☐ N
30	Cada incumplimiento detectado activa medidas correctoras sin demora indebida y se sigue hasta su cierre.	Art. 21.4	☐ S ☐ P ☐ N
31	Aplicas una línea base de ciberhigiene : bastionado, configuración segura, parcheo y mínima funcionalidad.	Art. 21.2.g	☐ S ☐ P ☐ N
32	Toda la plantilla recibe formación de concienciación , incluida la de phishing.	Art. 21.2.g	☐ S ☐ P ☐ N
33	Una política de criptografía define algoritmos aprobados y el ciclo de vida de las claves.	Art. 21.2.h	☐ S ☐ P ☐ N

34	Los datos se cifran en tránsito y en reposo cuando procede.	Art. 21.2.h	☐ S ☐ P ☐ N
35	La seguridad de los recursos humanos cubre altas, cambios y bajas, confidencialidad y verificaciones lícitas.	Art. 21.2.i	☐ S ☐ P ☐ N
36	El control de acceso sigue el mínimo privilegio, los accesos privilegiados están gestionados y los permisos se revisan periódicamente.	Art. 21.2.i	☐ S ☐ P ☐ N
37	Mantienes al día un inventario de activos : hardware, software, datos y responsables.	Art. 21.2.i	☐ S ☐ P ☐ N
38	La autenticación multifactor o continua protege el acceso remoto, administrativo y crítico.	Art. 21.2.j	☐ S ☐ P ☐ N
39	Cuando procede, hay comunicaciones de voz, vídeo y texto seguras y un sistema seguro de comunicaciones de emergencia .	Art. 21.2.j	☐ S ☐ P ☐ N
40	Has documentado por qué tus medidas son proporcionadas a tu exposición, tamaño, y probabilidad y gravedad de los incidentes.	Art. 21.1	☐ S ☐ P ☐ N
41	Si eres proveedor de DNS, TLD, nube, centro de datos, CDN, servicios gestionados (MSP/MSSP), mercado en línea, buscador, red social o servicios de confianza, tus medidas están mapeadas al Reglamento de Ejecución (UE) 2024/2690 .	Art. 21.5; Rgto. 2024/2690	☐ S ☐ P ☐ N

4 • Notificación de incidentes y supervisión

#	COMPROBACIÓN	REFERENCIA	ESTADO
42	Tus criterios de incidente significativo están escritos: perturbación operativa grave o pérdidas económicas, o daños considerables a terceros.	Art. 23.3; Rgto. 2024/2690	☐ S ☐ P ☐ N
43	Un procedimiento de alerta temprana en 24 horas fija quién decide, quién envía, a qué CSIRT y cómo funciona fuera de horario.	Art. 23.4.a	☐ S ☐ P ☐ N
44	Puedes emitir una notificación de incidente en 72 horas con evaluación inicial de gravedad, impacto e indicadores de compromiso.	Art. 23.4.b	☐ S ☐ P ☐ N
45	Puedes entregar un informe final en un mes (causa raíz, mitigación, impacto transfronterizo) o un informe de situación si el incidente sigue abierto.	Art. 23.4.d-e	☐ S ☐ P ☐ N
46	Sabes cómo informar a los destinatarios de tus servicios de incidentes y amenazas significativas. La notificación de brecha a la AEPD por el RGPD (72 h) corre en paralelo.	Art. 23.1-23.2; RGPD art. 33	☐ S ☐ P ☐ N
47	Tienes listo un paquete de evidencias para el supervisor: políticas documentadas, resultados de auditoría y pruebas de implantación.	Art. 32.2.e-g, 33.2.d-f	☐ S ☐ P ☐ N

Tu puntuación

Cuenta **2 puntos** por cada Sí, **1** por cada Parcial y **0** por cada No. Máximo: 94.

Puntos	Lectura
80–94	Base sólida. Céntrate en la calidad de las evidencias y en probar tu cadena de notificación de 24 h / 72 h.
50–79	Carencias reales. Prioriza gobernanza (sección 2) y notificación (sección 4): suelen ser lo más rápido de corregir.
0–49	Empieza por el ámbito, la aprobación del consejo y un procedimiento de incidentes. El siguiente paso es un análisis de carencias estructurado.

Estas franjas son una ayuda orientativa para priorizar, no una determinación de cumplimiento.

¿Quieres otra mirada sobre tus carencias?

Reserva una llamada y trae tu puntuación. Revisaremos tus tres secciones más débiles y qué corregir primero.

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

Fuentes

Directiva (UE) 2022/2555 (NIS2), DO L 333 de 27.12.2022 · Reglamento de Ejecución (UE) 2024/2690 de la Comisión · ENISA, *Technical Implementation Guidance on Cybersecurity Risk Management Measures*, v1.0, junio de 2025 · Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad (Ministerio del Interior, notificación TRIS 26686) · Comisión Europea, remisión al TJUE por NIS2, 8 de julio de 2026 · RD-ley 12/2018 y RD 43/2021.

Cambios europeos pendientes, sin fuerza de ley a 2026-10-07: el Digital Omnibus (punto único de notificación de incidentes, propuesto el 19 de noviembre de 2025) y las modificaciones de NIS2 COM(2026) 13 (propuestas el 20 de enero de 2026).

Este checklist es información general, no asesoramiento jurídico. Tus obligaciones dependen de tu sector, tamaño, Estado miembro y de la ley nacional definitiva.

© Angel Georgiev Sulev · Todos los derechos reservados