ie UNIVERSITY
CENTER FOR THE GOVERNANCE OF CHANGE

isms forum



ESTADO DE LA PREPARACIÓN NIS2 EN ESPAÑA

Madurez de gobierno de ciberseguridad en organizaciones esenciales e importantes

ÍNDICE

RESUMEN EJECUTIVO 03

1. INTRODUCCIÓN Y CONTEXTO 05
1.1 Por qué este estudio 05
1.2 Qué mide y qué no mide 05

2. EL MODELO DE MADUREZ 06

3. METODOLOGÍA 07
3.1 Muestra 07
3.2 Instrumento y validación 07
3.3 Clasificación objetiva de aplicabilidad 07
3.4 Bases de cálculo y tratamiento de respuestas incompletas 08

4. RESULTADOS 09
4.1 Panorama general de madurez 10
4.2 Hallazgo central: la meseta del nivel 2 11
4.3 Diferencias por clasificación, tamaño y sector 12
4.4 Madurez declarada frente a madurez según el modelo 13
4.5 La brecha de concienciación sobre el alcance de NIS2 13
4.6 Representación de la muestra y sesgo de cobertura 14

5. LECTURA ESTRATÉGICA 15

6. BENCHMARKING INTERNACIONAL 18
6.1 Contraste con las hipótesis del benchmarking 20

7. ANÁLISIS ECONÓMICO Y DE INVERSIÓN 23
7.1 Lo que cuesta cumplir: cinco marcos oficiales 24
7.2 Lo que cuesta no cumplir 25
7.3 El coste regulatorio directo: sanciones y responsabilidad personal 27
7.4 Lo que ningún sistema pone en precio 28
7.5 Qué invertir y cuánto: una propuesta 29
7.6 Datos propios: alcance y límite 31

8. LECTURA COMPLEMENTARIA Y CONVERGENCIA CUALITATIVA 32
8.1 Nota sobre el alcance de esta sección 33
8.2 Las fronteras del ámbito, vistas desde el texto libre 33
8.3 Quién responde: la función existe, el título no siempre 34
8.4 Certificarse ayuda, pero no basta 34
8.5 Convergencia con el panel de validación 35
8.6 La ambición a 24 meses 36

9. CONCLUSIONES Y RECOMENDACIONES 37

10. LIMITACIONES Y CAUTELAS METODOLÓGICAS 41
10.1 Trazabilidad de los tamaños de muestra(n) 42
10.2 Respuestas incompletas y posible sesgo 43

REFERENCIAS 44

ANEXO A — PERFILES SECTORIALES 45

ANEXO B — HIPÓTESIS DE TRABAJO DEL BENCHMARKING INTERNACIONAL 56

Investigador Principal:
Casimiro Juanes Calvo

RESUMEN EJECUTIVO

NIS2 ha trasladado la responsabilidad de la ciberseguridad al órgano de dirección. La pregunta ya no es solo si una organización tiene buenos controles técnicos, sino si su gobierno es capaz de entender, supervisar y dirigir el riesgo ciber. Este estudio mide, por primera vez en España y con un modelo validado por un panel de expertos, hasta qué punto las organizaciones están preparadas para ese papel, a partir de lo que describen sus propios responsables de seguridad.

Sobre una muestra de 209 organizaciones, cuatro hallazgos ordenan el diagnóstico.



01. Siete de cada diez organizaciones no alcanzan el umbral de cumplimiento básico.

El 72% se sitúa por debajo del nivel 3, y solo el 7% alcanza el nivel 4 o superior. En el modelo, el nivel 3 equivale a cumplimiento básico (suficiente para entidades importantes) y el nivel 4 a cumplimiento robusto (exigible a entidades esenciales). Entre las esenciales, solo el 12% está en ese nivel. La meseta está en el nivel 2, por debajo del umbral, no en él.



02. Lo que frena no es la tecnología, es el gobierno:

Integrar el riesgo ciber en la gestión empresarial y en la cultura corporativa. De las organizaciones ancladas en el nivel 2, el 77% lo está por su debilidad en gestión de riesgo empresarial o en cultura y capacidades. Las dimensiones técnicas, resiliencia operacional y gestión de terceros, son el único factor limitante en solo 3 de las 31 organizaciones frenadas por una sola dimensión. Bajando a las prácticas concretas, la más débil del estudio es la cuantificación: dos de cada tres organizaciones no ponen cifra económica a su riesgo ciber.



03. Hay una brecha de concienciación sobre el propio alcance de la norma.

El 30% de los participantes no se identifica con certeza como sujeto a NIS2. Al reconstruir su situación a partir de sector y tamaño, el 61% de ellos sí está en ámbito. De las 24 organizaciones que afirmaron que la norma no les aplica, 15 sí están sujetas, 11 de ellas como entidades esenciales.



04. Los responsables de seguridad se valoran por su media, no por su dimensión menos madura.

Dos de cada tres se sitúan por encima del nivel que les asigna el modelo, pero su autopercepción casi coincide con la media de sus cinco dimensiones. Lo que no ven es que basta una dimensión débil para fijar el nivel, y en casi cuatro de cada cinco de esos casos esa dimensión es el gobierno o el riesgo empresarial.

Dos datos completan el cuadro.

Certificarse ayuda, pero no basta: las organizaciones con ISO/IEC 27001 o ENS puntúan más alto en las cinco dimensiones, pero siguen de media en el nivel 2, y su menor ventaja está en la integración del riesgo en la gestión empresarial. Y la ambición existe: el 93% de las entidades esenciales quiere estar en el nivel 4 en dos años, cuando hoy lo está el 12%.

La lectura estratégica, para la muestra de este análisis (ver §4.6 sobre su representatividad), es directa: el cumplimiento de NIS2 en España no se juega solo en el centro de operaciones de seguridad, se juega en la sala del Consejo. La palanca está en integrar el riesgo ciber en la gestión empresarial, asentar una cultura de responsabilidad y llevar su supervisión al órgano de dirección, no en más tecnología.



1 INTRODUCCIÓN Y CONTEXTO

1.1 POR QUÉ ESTE ESTUDIO

La Directiva (UE) 2022/2555 (NIS2) amplía el perímetro de entidades obligadas y, sobre todo, sitúa en el órgano de dirección la responsabilidad de aprobar las medidas de gestión de riesgos de ciberseguridad que exige el artículo 21, supervisar su aplicación y responder de su incumplimiento (Art. 20). Entre esas medidas, el propio artículo 21 incluye políticas y procedimientos para evaluar su eficacia; para los proveedores de infraestructura y servicios digitales, el Reglamento de Ejecución (UE) 2024/2690 lo concreta técnicamente. En España, la transposición se articula a través de la futura Ley de Coordinación y Gobernanza de la Ciberseguridad: anteproyecto aprobado en primera vuelta, pendiente de segunda vuelta y de remisión a las Cortes, con el texto de enero de 2025 como última versión pública.

> A pesar de la relevancia regulatoria, no existía en España una medición del grado de preparación de los consejos y de las funciones de seguridad ante esta exigencia hecha con un modelo de madurez validado por expertos. Este estudio cubre ese vacío.

1.2 QUÉ MIDE Y QUÉ NO MIDE

El modelo que sustenta el estudio es una herramienta de diagnóstico de la madurez de gobierno de ciberseguridad. No es una checklist de cumplimiento legal ni una auditoría técnica. Evalúa la capacidad de una organización para gobernar el riesgo ciber, no la mera existencia de controles. Es complementaria de los marcos de certificación y verificación que las organizaciones españolas utilizan habitualmente, como el ENS, ISO/IEC 27001 o SOC 2: estos acreditan la existencia y el funcionamiento de los controles; el modelo evalúa la capacidad de gobierno que los dirige.

En este estudio, el modelo se aplica mediante un cuestionario que responde el responsable de seguridad de cada organización. Mide, por tanto, la madurez que la organización describe al contestar preguntas concretas sobre sus prácticas, no la verificada con evidencias por un tercero. Esa distinción es necesaria para leer los resultados, en particular la comparación entre autopercepción y modelo de §4.4.

En este informe, "Consejo" designa al órgano de dirección en el sentido del artículo 20 de NIS2: el consejo de administración en las empresas y el órgano superior de gobierno en las administraciones públicas y demás entidades.



2 EL MODELO DE MADUREZ

El modelo organiza la madurez en cinco dimensiones y cinco niveles. **Las dimensiones son:**

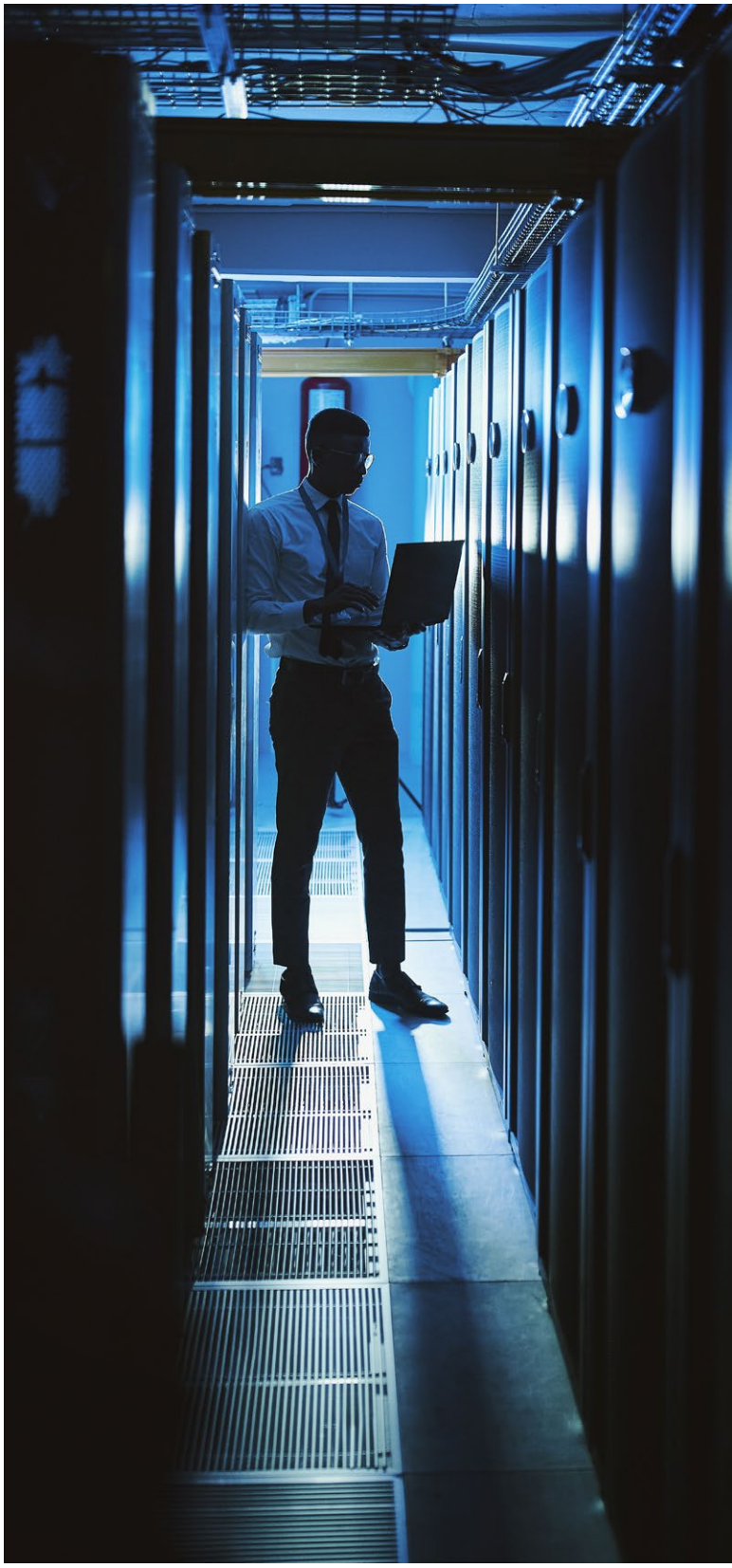
- gobierno y liderazgo **(D1)**
- gestión de riesgo empresarial **(D2)**
- resiliencia operacional y continuidad **(D3)**
- gestión de terceros y cadena de suministro **(D4)**
- cultura y capacidades organizacionales **(D5)**

Los niveles progresan de prácticas reactivas (N1) a una ciber-resiliencia como ventaja competitiva (N5).
El umbral regulatorio es explícito:

- **nivel 1** = inicial
- **nivel 2** = en desarrollo
- **nivel 3** = cumplimiento básico (Entidades Importantes)
- **nivel 4** = cumplimiento robusto (Entidades Esenciales)
- **nivel 5** = optimizado

Una característica metodológica define la lectura de todo el informe: **el nivel global de una organización es el mínimo de sus cinco dimensiones, no su promedio**. Una organización es tan madura como su dimensión más débil. Esta regla, lejos de ser una penalización arbitraria, refleja que el gobierno del riesgo no admite eslabones débiles: una cadena de suministro impecable no compensa un consejo que no supervisa.

Los niveles 4 y 5 incorporan una lógica de gobernanza orientada a resultados (King IV, 2016) y de resiliencia anticipatoria (Hollnagel, 2006; Woods, 2015): no basta con tener procesos, hay que demostrar que producen resultados observables y que la organización anticipa disrupciones.



El detalle de los descriptores de cada subdimensión y nivel se recoge en el documento canónico del modelo: NIS2 · Modelo de Madurez de Gobierno de Ciberseguridad v2.0 (Center for the Governance of Change, IE University, e ISMS Forum, abril de 2026), disponible en www.ismsforum.es/ficheros/descargas/proyecto-nis21778078842.pdf

3 | METODOLOGÍA

3.1 MUESTRA

El estudio recoge **209 respuestas**: 144 a través de ISMS Forum, 48 por canal abierto, 10 de panel experto y 7 por contacto directo; el panel experto se incluye con etiqueta y su efecto sobre las medias agregadas es de 0,02 puntos como máximo. **Por autoclasificación NIS2**: 86 esenciales, 61 importantes, 31 "probable", 24 "no aplica" y 7 "no sabe/no responde".

Por tamaño, según las bandas de empleados del cuestionario: 36 organizaciones con menos de 250 empleados, 82 entre 250 y 2.500, 50 entre 2.501 y 10.000 y 41 con más de 10.000. El informe las denomina pequeñas, medianas, grandes y muy grandes; son etiquetas de la muestra y no coinciden con la definición europea de pyme (Recomendación 2003/361/CE), en la que 250 empleados ya marcan la gran empresa. La fotografía general de madurez se reporta sobre el total. Los cortes por clasificación esencial/importante se reportan sobre las 147 organizaciones que portan esa etiqueta.

> Un modelo validado por un panel de 12 expertos. Un cuestionario con 209 respuestas de organizaciones de diversos sectores en España. Una regla de base: cada organización es tan madura como su dimensión menos madura. Se mide la madurez que describe el responsable de seguridad, no la verificada con evidencias.

3.2 INSTRUMENTO Y VALIDACIÓN

El cuestionario consta de un bloque demográfico, once preguntas de madurez y un bloque final de autoevaluación y ambición a 24 meses. Las preguntas de madurez se asignan a las dimensiones del modelo: tres a gobierno y liderazgo (D1: línea de reporte del responsable de seguridad, información al Consejo y participación en decisiones estratégicas) y dos a cada una de las otras cuatro. Cada pregunta ofrece seis respuestas ordenadas, de 0 (ausencia de la práctica) a 5; las respuestas 1 a 5 corresponden a los niveles 1 a 5 del modelo y la respuesta 0 se asimila al nivel 1. La puntuación de cada dimensión es la media de sus preguntas en esa escala. El modelo fue validado por un panel de 12 expertos mediante Content Validity Index, con un S-CVI/Ave global de 0,917 (excelente según los umbrales de Lynn 1986 y Polit & Beck 2006).

3.3 CLASIFICACIÓN OBJETIVA DE APLICABILIDAD

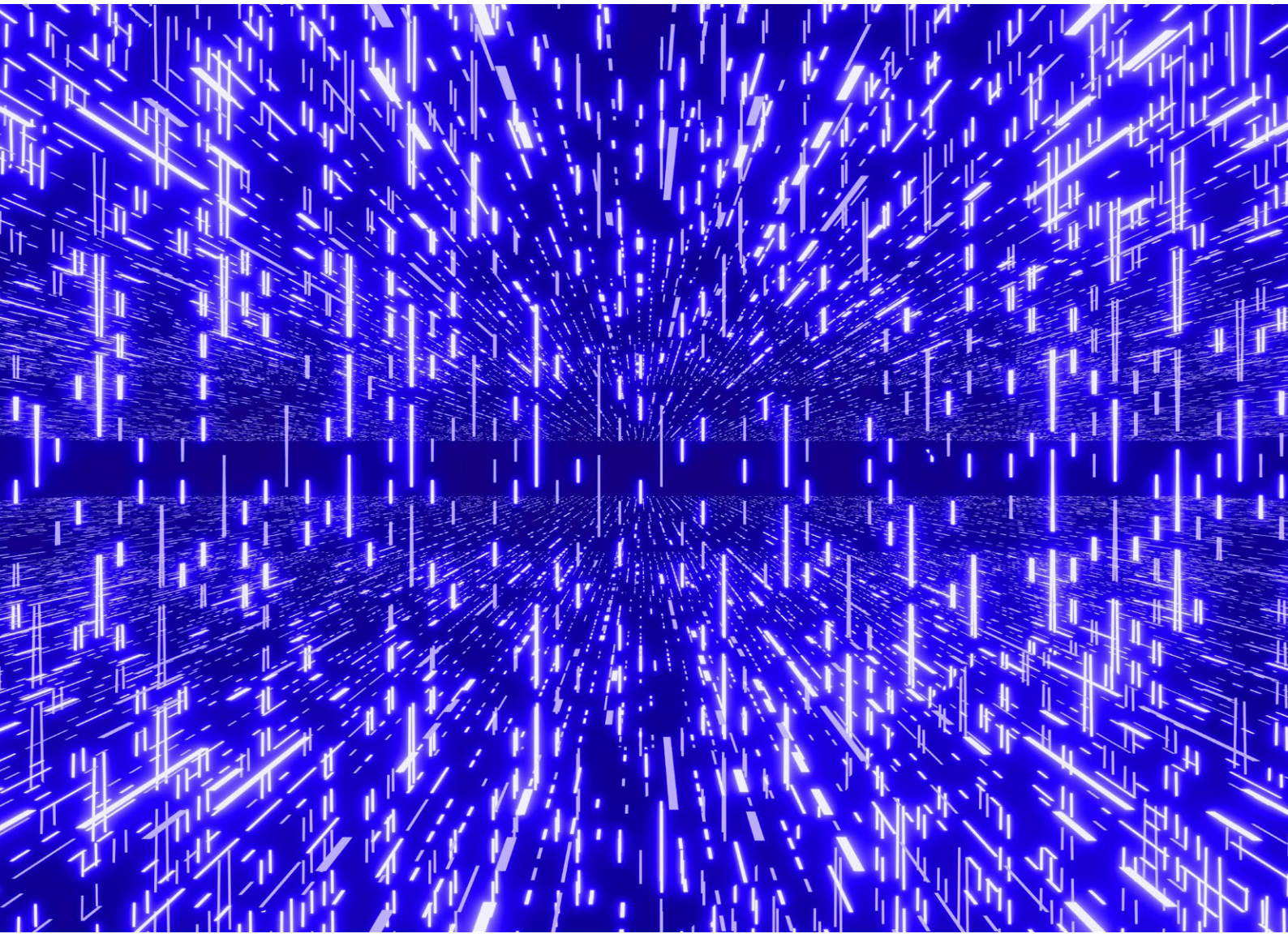
Para distinguir entre madurez declarada y aplicabilidad real, se reconstruyó la sujeción a NIS2 de cada organización a partir de su sector (Anexo I o II de la directiva), número de empleados y facturación. NIS2 se aplica a partir de la mediana empresa (50 o más empleados, o más de 10 M€ de facturación). Como la encuesta recoge el tamaño en bandas (menos de 25, 26–250, 250 o más), se considera en ámbito con certeza a quien declara 250 o más empleados o más de 10 M€; es esencial si es grande (250 o más empleados o más de 50 M€) en un sector del Anexo I, e importante en el resto de casos en ámbito. La administración pública es esencial con independencia del tamaño. En la banda de 26 a 250, que cruza el umbral legal, decide la facturación; sin ella, el caso se marca como indeterminado.

3.4 BASES DE CÁLCULO Y TRATAMIENTO DE RESPUESTAS INCOMPLETAS

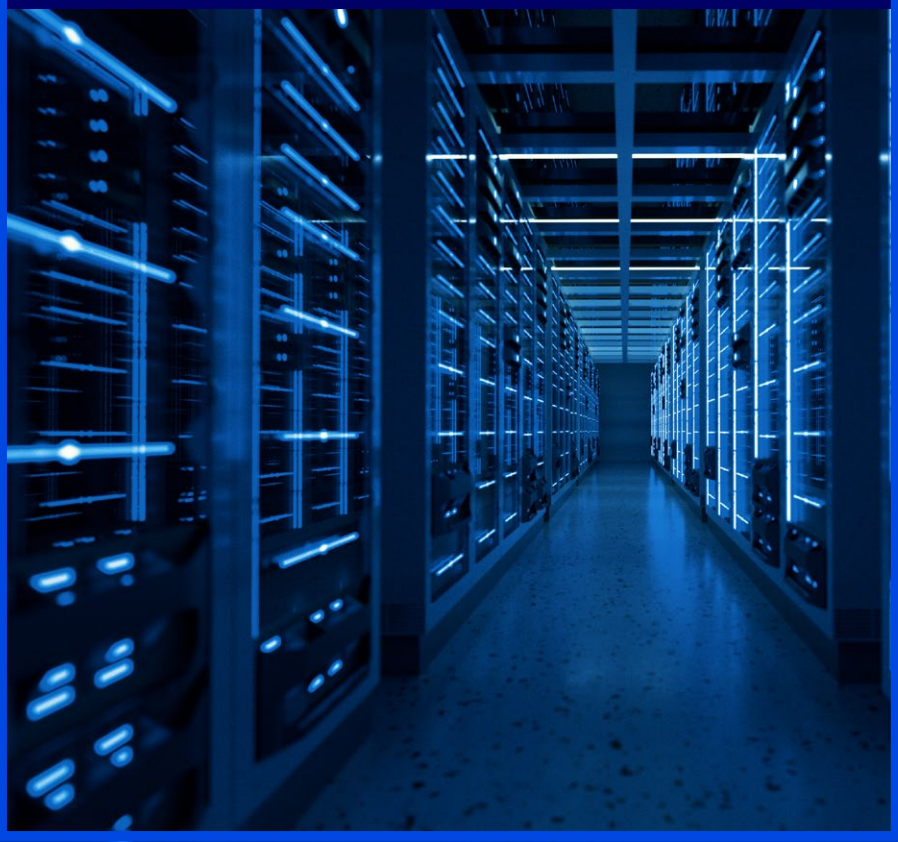
La encuesta se respondió de forma voluntaria y sin obligación de completar todos los bloques, de modo que el número de respuestas disponibles varía según la pregunta. El estudio no imputa valores ausentes ni descarta respondentes: cada análisis se calcula sobre quienes contestaron las preguntas que ese análisis necesita, y el informe indica la base muestral cada vez que difiere del total.

Se aplican tres bases. Los análisis de una sola dimensión (medias y distribuciones de D1 a D5) utilizan a todos los respondentes que completaron esa dimensión. El nivel global de madurez se calcula únicamente para quienes completaron las cinco, porque el modelo lo define como el mínimo de las cinco dimensiones y ese mínimo no puede determinarse si falta alguna: son 169 de las 209 respuestas. Los cruces entre dos variables, como el contraste entre nivel global y madurez autopercibida, se calculan sobre quienes respondieron ambas, lo que reduce ligeramente la base respecto al nivel global.

El patrón de respuestas ausentes es progresivo, propio del abandono del cuestionario: faltan 16 respuestas en D1, 24 en D2, 29 en D3, 31 en D4 y 40 en D5. De las 40 respuestas sin nivel global, 16 no contestaron ninguna dimensión y solo 9 dejaron una sola sin responder. La sección 10 analiza las implicaciones de este patrón.



RESULTADOS





04

4 | RESULTADOS

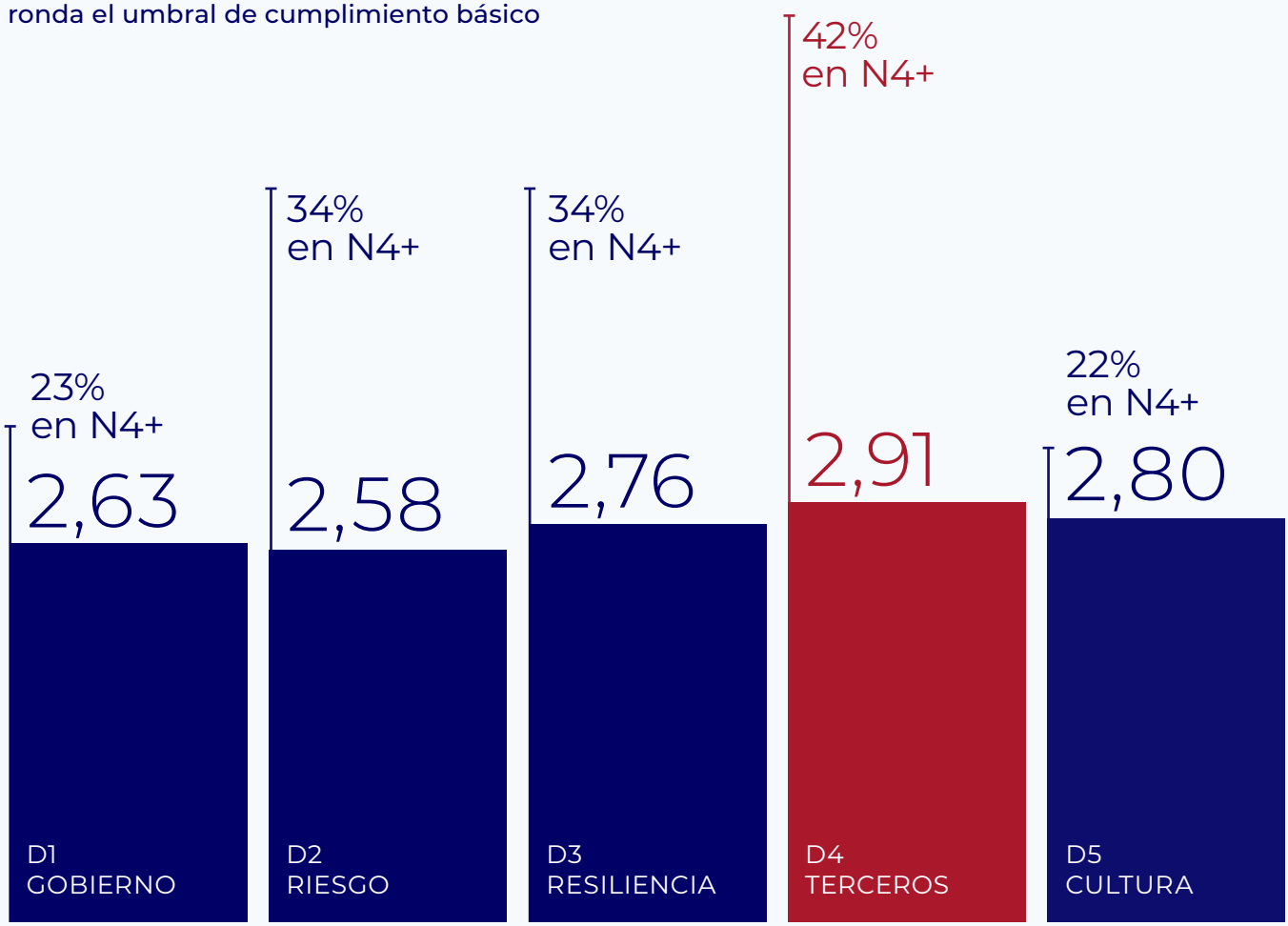
4.1 PANORAMA GENERAL DE MADUREZ

A nivel de dimensión, la madurez se sitúa en torno al nivel 3, el umbral de cumplimiento básico. La gestión de terceros (D4) es la más alta, con una media de 2,91 sobre 5 y un 42% de organizaciones en nivel 4 o superior. La gestión de riesgo empresarial (D2) es la más baja, con media 2,58 y un 34% en nivel 4+.

Sin embargo, el **nivel global se desploma**: solo el 7% alcanza N4+, y el 72% no llega al nivel 3, el umbral de cumplimiento básico. La distribución global (n = 169): 45 en N1, 77 en N2, 36 en N3, 8 en N4 y 3 en N5. El nivel 2 es la moda.

FIGURA 1.

Dimensión a dimensión, la madurez ronda el umbral de cumplimiento básico



4.2 HALLAZGO CENTRAL: LA MESETA DEL NIVEL 2

La distancia entre una madurez dimensional aceptable y un nivel global bajo se explica por la regla del mínimo: basta una dimensión rezagada para fijar el nivel de toda la organización.

De las 77 organizaciones ancladas en nivel 2, la dimensión que actúa como restricción es la siguiente:

TABLA 1.

El riesgo empresarial es el freno más frecuente

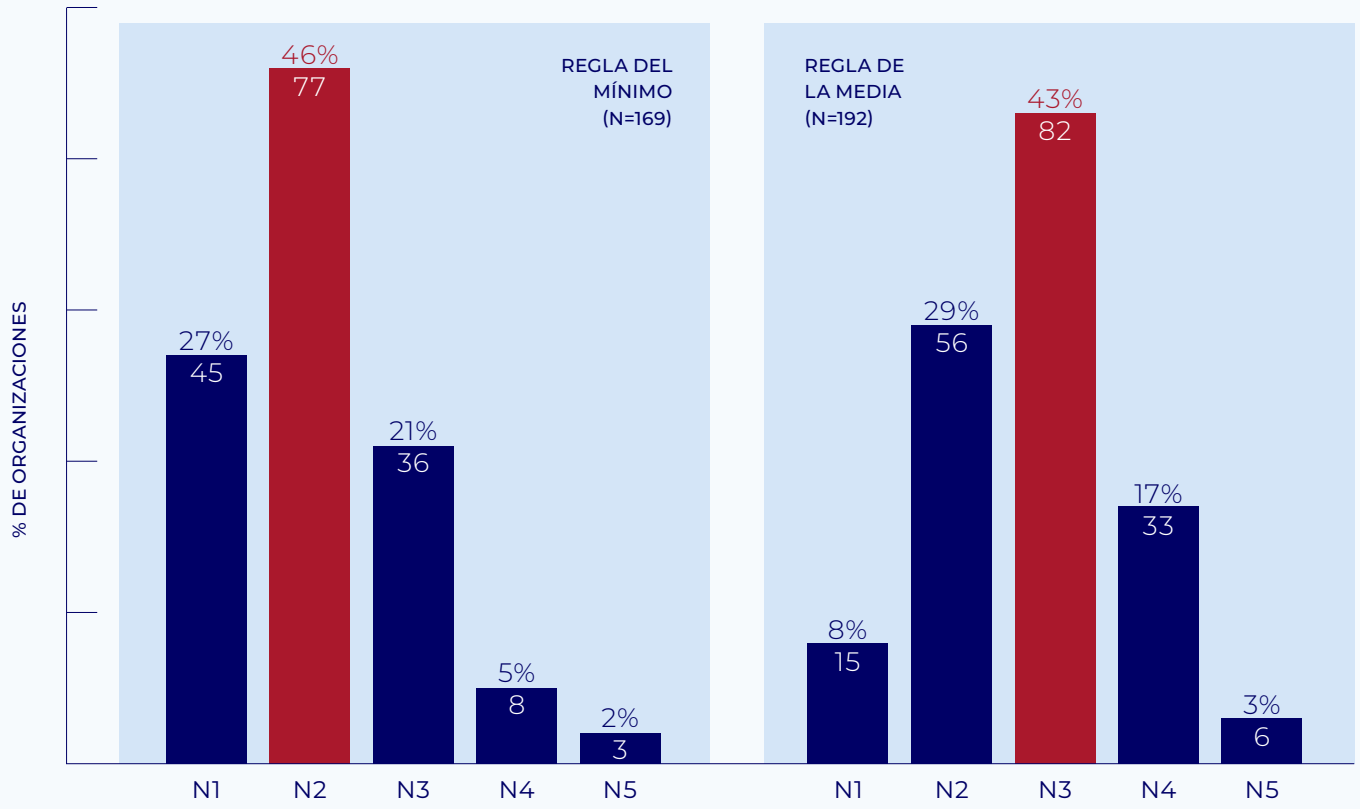
Dimensión	Limita en N2	Es el único cuello de botella
D1 Gobierno	39%	6
D2 Gestión de riesgo	58%	14
D3 Resiliencia	31%	2
D4 Terceros	31%	1
D5 Cultura	35%	8

La gestión de riesgo empresarial es el freno principal: limita al 58% de las organizaciones en nivel 2 y es el único cuello de botella en 14 de los 31 casos en que una sola dimensión las frena. Le siguen la cultura y las capacidades (8 casos) y el gobierno y liderazgo (6). Las dimensiones técnicas, D3 y D4, son el único factor limitante en 3 de esos 31 casos. En conjunto, el 77% de las organizaciones en nivel 2 está limitado por riesgo empresarial o por cultura, y el 90% si se añade el gobierno y liderazgo. Un matiz: 46 de las 77 organizaciones están limitadas por dos o más dimensiones a la vez, de modo que para una buena parte no se trata de un único eslabón débil sino de inmadurez en varios frentes. Pero el frente que más reaparece es el riesgo empresarial.

La conclusión estratégica: **el nivel 2 no es un techo de capacidad, es una meseta de consistencia**. Más de la mitad ya tiene sus dos dimensiones técnicas en el nivel 3 o por encima. Su palanca es integrar el riesgo ciber en la gestión empresarial y en la cultura corporativa. El cuello de botella vive en territorio de gobierno, no de tecnología.

FIGURA 2.

La dimensión menos madura decide: siete de cada diez no llegan al nivel 3



4.3 DIFERENCIAS POR CLASIFICACIÓN, TAMAÑO Y SECTOR

Las entidades esenciales superan a las importantes en todas las dimensiones; la mayor diferencia está en gobierno (D1, 0,4 puntos), no en las dimensiones técnicas. El 12% de las esenciales alcanza N4+ (9 de 73); entre las importantes, solo una de 48. La brecha es de exigencia y de atención del Consejo.

La madurez da un salto de 2,55 a 2,97 entre las organizaciones de 250 a 2.500 empleados y las de 2.501 a 10.000: el mayor salto se produce en torno a los 2.500 empleados. La madurez crece con el tamaño y los niveles más altos se concentran en las organizaciones de más de 10.000 empleados, coherente con el principio de proporcionalidad del modelo y de la directiva (Art. 21.1).

Por sector, considerando solo los de Anexo I/II con al menos 10 respuestas, las medias van de 2,48 a 3,15 sobre 5. Banca y Finanzas, Infraestructura digital/TIC y Transporte forman la banda alta; Manufactura, AAPP y Alimentación, la baja, separadas entre sí por apenas una décima, dentro del margen de error.

> La madurez crece con el tamaño: las organizaciones de más de 10.000 empleados superan en casi un punto a las de menos de 250. Entre sectores, las diferencias son menores que entre tamaños, y ninguno alcanza de media el nivel 4.

FIGURA 3.

Las diferencias entre sectores son pequeñas: ninguno alcanza de media el nivel 4

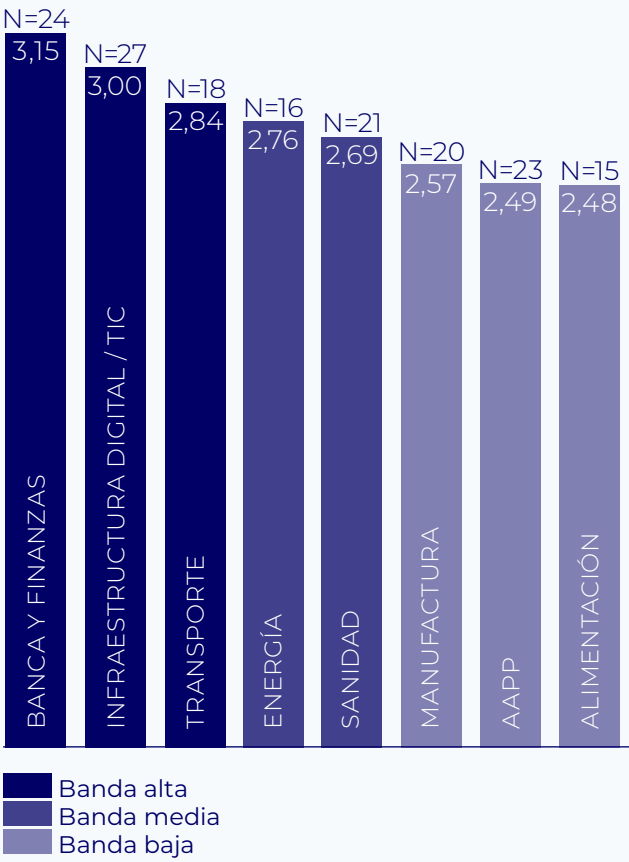
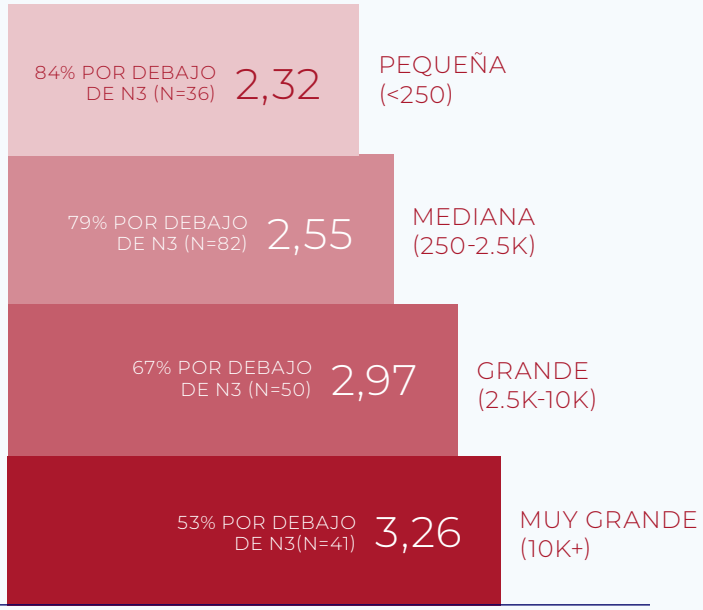


FIGURA 4.

La madurez crece con el tamaño, y el mayor salto llega a partir de 2.500 empleados



4.4 MADUREZ DECLARADA FRENTE A MADUREZ SEGÚN EL MODELO

Se comparó la autopercepción de cada responsable de seguridad con el nivel que le asigna el modelo (n = 166). La autopercepción media (2,9) supera a la del modelo (2,1) en 0,8 puntos: el 66% se sitúa por encima del nivel del modelo, el 30% coincide y el 4% queda por debajo.

La diferencia no indica que los responsables de seguridad inflen su madurez. Frente a la media de sus cinco dimensiones, la autopercepción casi coincide (+0,2; el 61% coincide exactamente). Lo que no recoge es la dimensión menos madura: en 86 de los 110 casos que se sitúan por encima, el nivel lo fija el gobierno o el riesgo empresarial. Los responsables de seguridad se valoran por su media; el modelo, por su dimensión menos madura.

Donde la diferencia pesa es en el umbral. De las 24 entidades esenciales que se sitúan en N4 o más, el modelo lo confirma en 8. Entre las importantes, 20 de las 28 que se sitúan en N3 o más no alcanzan el umbral básico según el modelo. No es autocomplacencia: es una brecha en las capacidades de gobierno que la norma exige.

4.5 LA BRECHA DE CONCIENCIACIÓN SOBRE EL ALCANCE DE NIS2

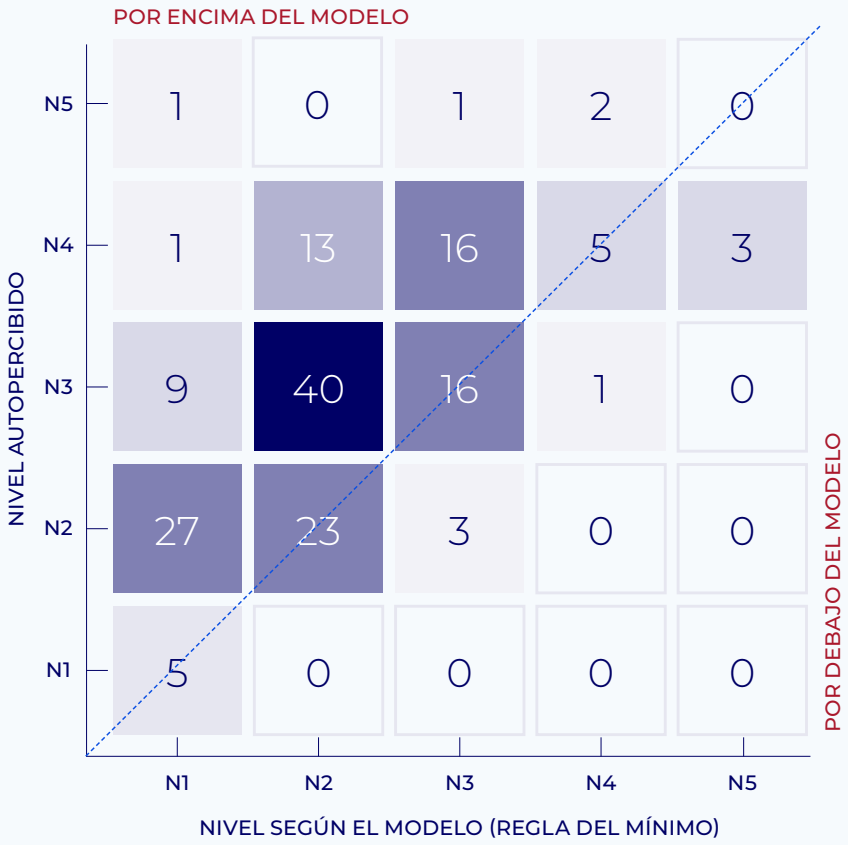
El 30% de los participantes (62 de 209) no se identifica con certeza como sujeto a NIS2. La reconstrucción objetiva muestra que el 61% de ellos (38 organizaciones) sí está en ámbito.

El caso más revelador son los 24 que afirmaron que la norma no les aplica: 15 sí están sujetos, 11 de ellos como entidades esenciales. Organizaciones que se creen exentas y son, de hecho, las más obligadas.

No toda la incertidumbre es desconocimiento. Una parte de quienes marcaron “otro” son aseguradoras, correctamente fuera de NIS2, porque el seguro no figura en sus anexos. Esa distinción, lejos de debilitar el hallazgo, lo refuerza: el grupo realmente preocupante son las entidades en sectores cubiertos que no saben que lo están.

FIGURA 5.

Los responsables de seguridad se valoran por su media; el modelo, por su dimensión menos madura



4.6 REPRESENTACIÓN DE LA MUESTRA Y SESGO DE COBERTURA

La muestra cubre con solidez varios sectores NIS2: Infraestructura Digital / TIC, Banca y Finanzas, AAPP, Sanidad, Manufactura alcanzan o superan las 20 respuestas, y Transporte, Energía, Alimentación se mueven entre 10 y 20. En cambio, quedan finos sectores que en buena parte coinciden con la zona de riesgo de ENISA (madurez por debajo de su criticidad), señaladamente agua e investigación: Otros NIS2 (n=2), Investigación (n=5), Agua (n=8). Son justo donde la madurez europea va por detrás de la exposición y donde menos podemos afirmar todavía con estos datos.

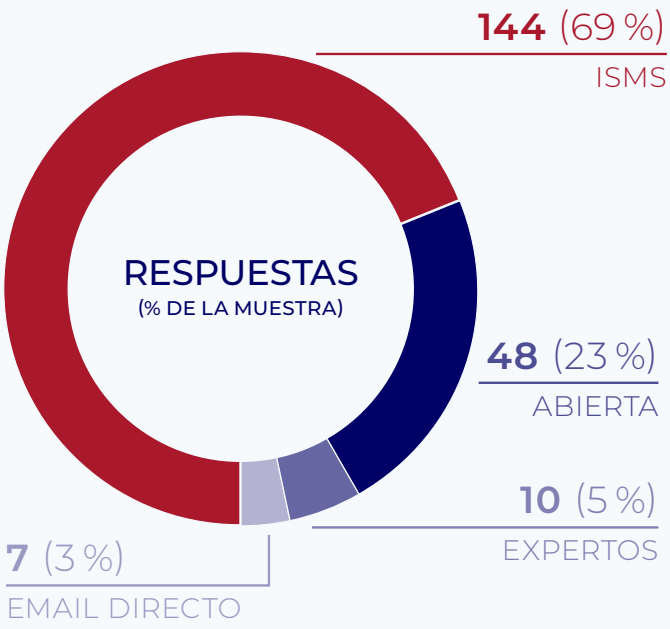
Hay además un sesgo de cobertura que conviene nombrar. El 69% de las respuestas llega por ISMS Forum, es decir, organizaciones que ya tienen una función de seguridad constituida. Solo el 17% son organizaciones pequeñas, y un 19% no completó todas las dimensiones, señal de que no siempre existe la estructura interna para responder a un diagnóstico de gobierno. A esto se suma que el 30% no se identifica con certeza como sujeto a NIS2. El sesgo apunta en una sola dirección: quienes no respondieron, o no pudieron, son sistemáticamente los menos maduros.

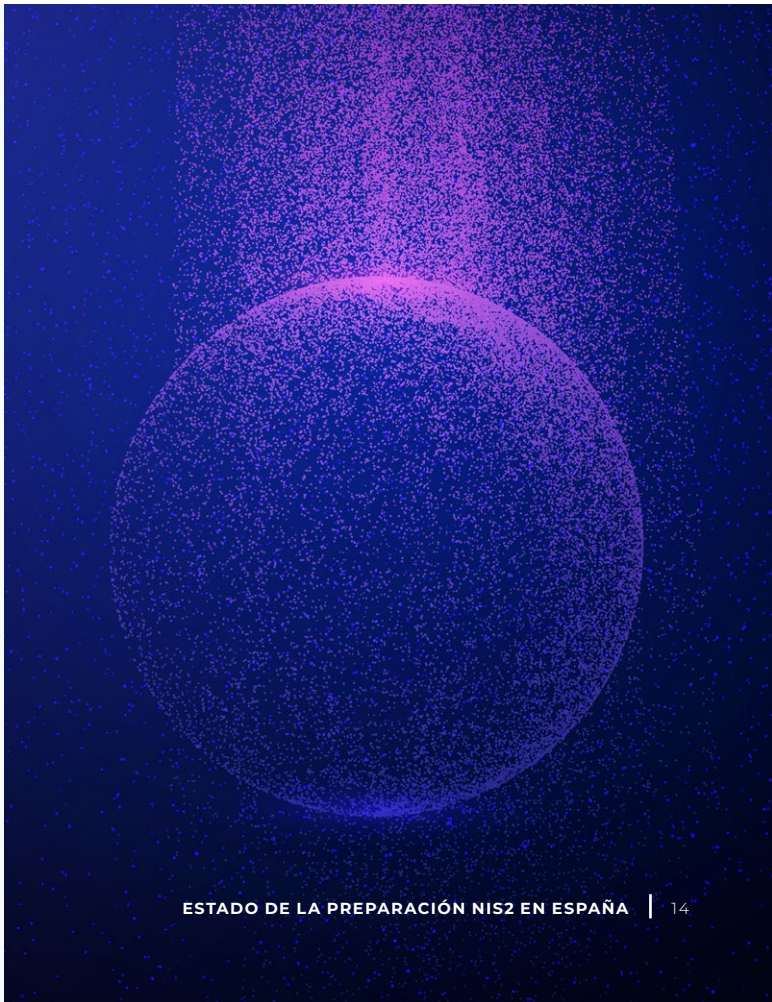
La consecuencia es doble. Primero, la fotografía nacional real es probablemente menos madura que la que refleja esta muestra, porque la cola no alcanzada concentra a los menos preparados. Segundo, el propio diseño del estudio debe ampliarse: llegar a más sectores infrarrepresentados (agua, investigación, entidades pequeñas) y, sobre todo, a las organizaciones que aún no saben que están en ámbito o que carecen de estructura para responder.

> 209 respuestas frente a las cerca de 5.760 entidades que el Gobierno estima sujetas a NIS2 (Memoria del Análisis de Impacto Normativo del anteproyecto de ley). Esa cola silenciosa no es ruido estadístico: es el núcleo del problema de preparación NIS2 en España.

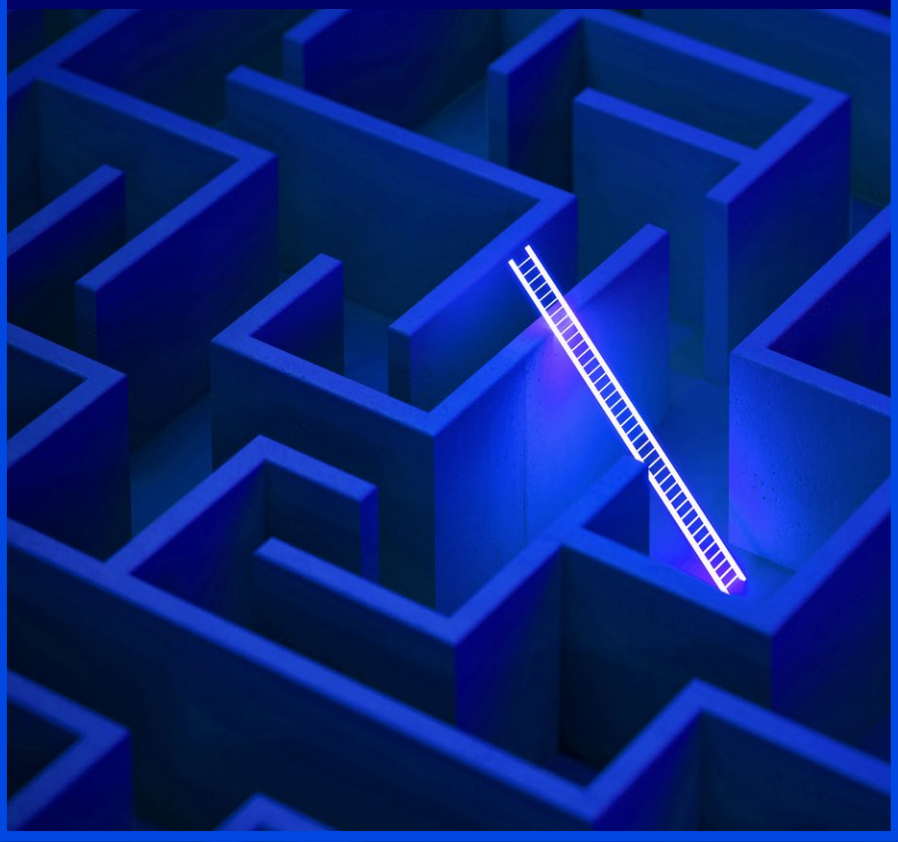
FIGURA 6.

Siete de cada diez respuestas llegan a través de ISMS Forum





LECTURA ESTRATÉGICA



05

5 | LECTURA ESTRATÉGICA

Para el equipo ejecutivo, y en particular para el CISO.

El informe ofrece un argumento basado en evidencia para reorientar la inversión. Si la organización está anclada en nivel 2, el retorno marginal no está en más herramientas, sino en integrar el riesgo ciber en el marco de gestión empresarial (D2) y en la cultura y las capacidades de la organización (D5). Conviene subrayar que ninguna de esas dos palancas está en manos del responsable de seguridad: la primera pertenece al marco de gestión de riesgos corporativo y la segunda a la política de personas de la compañía. Reorientar la inversión hacia ellas es, por tanto, una decisión del comité de dirección, y el lenguaje en que se expresa es el que el Consejo ya entiende.

Para el Consejo.

NIS2 hace al órgano de dirección responsable. Este estudio muestra que la barrera para el cumplimiento, incluso el básico, no es técnica sino de gobierno, justo el terreno donde el Consejo tiene competencia y responsabilidad indelegable.

El artículo 20 de la Directiva exige tres cosas al órgano de dirección: aprobar las medidas de gestión de riesgos, supervisar su implantación efectiva y recibir formación que permita a sus miembros identificar riesgos y evaluar las prácticas de gestión. No son obligaciones nuevas en su naturaleza, sino la concreción en materia de ciberseguridad de un deber que el derecho societario español ya impone. El deber de diligencia del administrador incluye recabar la información adecuada y necesaria para el desempeño del cargo, y la protección de la discrecionalidad empresarial, que ampara al consejero frente a decisiones de negocio que salen mal, se condiciona a que haya actuado con información suficiente y con arreglo a un procedimiento de decisión adecuado (arts. 225 y 226 de la Ley de Sociedades de Capital). Trasladado a este ámbito, la consecuencia es directa: **la evidencia de que el Consejo fue informado, deliberó y decidió sobre el riesgo ciber no es solo una exigencia de cumplimiento, es el presupuesto de la protección del propio consejero.** Un Consejo que no puede demostrar cómo supervisó carece del elemento que hace defendible su decisión.

De ahí que el modelo de madurez esté diseñado para evaluar la capacidad demostrada y no la declaración formal. La distinción procede de la lógica *apply and explain* del King IV Code (2016), que sustituye al clásico *comply or explain*: el principio de gobierno no se cumple declarando adhesión, sino explicando cómo se ha aplicado y qué resultado ha producido. Es exactamente la diferencia que separa el nivel 3 del nivel 4 en este modelo. Una organización en nivel 3 tiene procesos documentados y reporta al Consejo con regularidad; una organización en nivel 4 puede demostrar, con evidencia observable, que esa supervisión modifica decisiones. Para el consejero, esa diferencia no es académica: es la distancia entre poder acreditar la diligencia y no poder hacerlo.



Para el regulador.

La brecha de concienciación sobre el alcance sugiere que el esfuerzo de comunicación de INCIBE y las autoridades competentes debería priorizar la identificación de entidades sujetas, no solo la difusión de requisitos. En la ventana pre-transposición actual, llegar a la cola no concienciada (sectores como agua o investigación, y entidades sin función de seguridad) es la palanca de mayor impacto antes de que el enforcement active el cumplimiento reactivo.



La economía de la no gobernanza.

Conviene nombrar quién se beneficia de la ausencia de gobernanza y dónde acaba el riesgo, porque reformula el coste de la inacción. Lo que los datos muestran es que el freno no es de capacidad técnica sino de gobierno: el 77% de las organizaciones ancladas en nivel 2 lo están por riesgo (D2) o cultura (D5), no por tecnología. Hay, por tanto, organizaciones con controles desplegados pero sin la supervisión del Consejo, la integración del riesgo o la cultura que los gobiernan. Ese estado de "no gobernanza" no es un vacío neutro: tiene beneficiarios y tiene quien soporta el riesgo.

En el corto plazo, la no gobernanza es localmente más barata y cómoda. Quien no gobierna se ahorra la fricción de la atención del Consejo, de cuantificar el riesgo y de supervisar a sus terceros; el beneficiario inmediato es quien aplaza ese coste. Pero el riesgo no desaparece, se transfiere y se difiere: recae sobre el propio Consejo, ahora personalmente responsable (Art. 20); sobre clientes y cadena de suministro, por concentración y contagio (D4); y sobre el conjunto del sector, como externalidad que nadie eligió asumir.

Ahí está el argumento que da la vuelta al coste de la inacción. La gobernanza parece un coste; la no gobernanza es un coste mayor, diferido y externalizado, que además aterriza sobre quien menos capacidad tiene de absorberlo. Esa asimetría (barato de evitar, caro de soportar, y soportado por terceros) es la razón de fondo por la que NIS2 responsabiliza al Consejo y no al CISO: para internalizar un coste que el mercado infravalora.

BENCHMARKING INTERNACIONAL



06

6 | BENCHMARKING INTERNACIONAL

Los hallazgos españoles no son una anomalía: encajan en el patrón europeo, con dos matices propios que merecen lectura.

Contexto regulatorio diferencial.
España mide su madurez en una ventana pre-enforcement: la transposición está pendiente: anteproyecto aprobado en primera vuelta, pendiente de segunda vuelta y de remisión a las Cortes, mientras Alemania ya opera bajo supervisión activa del BSI desde diciembre de 2025 y Francia mantiene su transposición en trámite parlamentario. Esto convierte al estudio en una línea base de madurez intrínseca, no forzada por inspecciones, lo que tiene valor metodológico: captura el estado real antes del efecto distorsionador del compliance reactivo.

Nivel de preparación.
Que solo el 7% alcance N4+, y que el 72% no llegue al nivel 3, es coherente con lo que reportan las encuestas europeas disponibles, aunque sus escalas y muestras no permiten una comparación directa: IDC (2026, n=2.000) sitúa un 14% de las organizaciones en su nivel de preparación más alto, CyberSmart (2026, n=670) un 16% plenamente conformes, y Cisco (2025) solo un 4% de empresas "maduras" a escala mundial. En todas, la preparación plena es minoritaria.

Jerarquía sectorial.
El benchmark sectorial más autorizado, ENISA NIS360 (2024 y 2026), sitúa en alta madurez a banca, electricidad y telecomunicaciones, y en zona de riesgo (madurez por debajo de su criticidad) a salud, agua, administración pública, gestión de servicios TIC y espacio. Nuestros datos coinciden en parte con esa jerarquía: Banca y Finanzas está en la banda alta y AAPP en la baja. No coinciden en todo: Infraestructura digital/TIC aparece aquí en la banda alta, y Alimentación y Manufactura, en la baja, no figuran en la zona de riesgo de ENISA.

Concienciación.
Aquí está el dato español más llamativo. En nuestra muestra, el 18% de los participantes está en ámbito sin identificarse con certeza como sujeto a la norma, y el 30% no se identifica con certeza como sujeto, esté o no en ámbito. Es consistente con una España todavía pre-transposición.



6.1 CONTRASTE CON LAS HIPÓTESIS DEL BENCHMARKING

6.1.1 Origen y alcance del contraste

Antes de la medición nacional, este proyecto realizó un benchmarking internacional que revisó la evidencia europea disponible sobre madurez y gobierno de la ciberseguridad y la contrastó con el diseño del modelo. De ese trabajo se derivaron doce hipótesis sobre cómo se comportaría el tejido empresarial español frente al patrón europeo, formuladas antes de conocer ningún resultado y asociadas cada una a la pregunta del cuestionario que permitiría contrastarla. Las fuentes de las que proceden, dimensión por dimensión, se recogen en el ▶Anexo B.

Someterlas ahora al dato es una exigencia de método: una hipótesis que no se expone a refutación no aporta conocimiento, y las que fallan enseñan más que las que aciertan. Conviene señalar el alcance de lo que sigue. Los veredictos se refieren a esta muestra, a su composición sectorial y de tamaño y al momento en que se recogió; no son conclusiones definitivas sobre el tejido empresarial español. Mediciones futuras, con muestras distintas o con el régimen de transposición ya en vigor, pueden modificar cualquiera de ellos, y algunas de las hipótesis que aquí quedan abiertas requieren preguntas que este instrumento no incluye.

6.1.2 Hipótesis confirmadas

H1 — La madurez media se situaría entre los niveles 2 y 3, con predominio del nivel 2 en las entidades importantes. Se confirma: la media global es 2,1, el nivel 2 es la moda y, entre las entidades importantes, el 83% se sitúa en los niveles 1 o 2.

H2 — El posicionamiento del responsable de seguridad sigue anclado en la estructura técnica. Se confirma. A la pregunta sobre a quién reporta directamente la máxima autoridad de ciberseguridad, el 52% responde que a un directivo funcional (CIO, CTO, COO) o a un responsable técnico, y solo el 26% al primer ejecutivo, al comité de dirección o al Consejo. La mayoría se sitúa así en el nivel 2 de la subdimensión de posicionamiento e influencia, o por debajo.

H4 — La cuantificación económica del riesgo será excepcional. Se confirma con holgura: el 44% evalúa el impacto únicamente en términos cualitativos de bajo, medio y alto, y apenas el 5% alcanza la cuantificación monetaria integrada en modelos de estrés que el modelo asocia a los niveles superiores. Es el mayor déficit individual detectado en toda la medición.

H5 — La participación del responsable de seguridad en las decisiones estratégicas sería menor en las entidades importantes que en las esenciales. Se confirma. A la pregunta sobre cómo participa el responsable de seguridad en las decisiones estratégicas de su organización, el 30% de las entidades esenciales responde que participa en la mayoría de ellas o al mismo nivel que otros directivos, frente al 19% de las importantes. En estas, el 53% no participa, solo es consultado de forma puntual o no tiene un responsable de seguridad definido (39% en las esenciales). La diferencia se refleja también en la dimensión de gobierno y liderazgo, 0,43 puntos a favor de las esenciales. El dato describe la participación tal como la declara el responsable de seguridad, no su peso efectivo en las decisiones.

H10 —El responsable de seguridad sobreestimaría la madurez de su organización. Se confirma frente a la regla del modelo, con un matiz que cambia su lectura: el 66% se sitúa por encima del nivel que le asigna el modelo, el 30% coincide y el 4% queda por debajo. Frente a la media de sus propias dimensiones, la autopercepción casi coincide (+0,2). No es autocomplacencia: el responsable de seguridad se valora por su media, y el modelo, por su dimensión menos madura (§4.4).

6.1.3 Hipótesis refutadas

- **H6 — La continuidad de negocio sería un área de déficit generalizado.** No se sostiene: el 63% dispone de un análisis de impacto documentado que fundamenta sus planes de continuidad y recuperación, y la resiliencia operacional se sitúa por encima de la media de las dimensiones.
- **H7 — Los ejercicios de crisis serían infrecuentes.** No se sostiene: el 59% realiza ejercicios al menos anuales, y más de un tercio (36%) con participación de la alta dirección o del Consejo. Solo el 19% no ha realizado ninguno o responde de forma improvisada.
- **H8 — El inventario de terceros críticos sería informal en la mayoría.** No se sostiene: el 65% mantiene identificados a sus proveedores críticos con criterios definidos o con inventario continuo integrado en los procesos de compras, y solo el 9% carece de inventario formal.

6.1.4 Hipótesis sin datos concluyentes

- **H3 — La alineación entre el responsable de seguridad y el Consejo sería de las más bajas del entorno europeo.** No es contrastable por construcción: este estudio recoge la percepción del responsable de seguridad y no la del órgano de gobierno, de modo que puede describir cómo el primero ve la supervisión, pero no medir la distancia entre ambas percepciones. Cerrar esa brecha exige un instrumento dirigido al Consejo.
- **H9 La evaluación de ciberseguridad de terceros sería ad hoc o inexistente en la mayoría de las entidades importantes.** Se sostiene parcialmente. En su exigencia alta el déficit es claro, ya que solo el 8% dispone de un programa completo con monitorización continua y planes de sustitución; pero el 39% realiza al menos cuestionarios periódicos con cláusulas contractuales, de modo que la formulación original resulta demasiado severa.
- **H11 — Los consejos asumirían formalmente la supervisión de nuevos riesgos más rápido que su capacidad real de ejercerla.** Esta hipótesis procede de la observación, en estudios internacionales sobre supervisión de la inteligencia artificial en los consejos de administración, de que la asunción formal de nuevos cometidos tiende a adelantarse a la capacidad efectiva de desempeñarlos. Trasladada a la ciberseguridad, la frecuencia con que el Consejo recibe información supera al posicionamiento del responsable de seguridad en 0,22 puntos; la supervisión formal puntúa por encima en el 44% de los casos y por debajo en el 34%. Es un indicio compatible con la hipótesis, pero el instrumento no permite afirmarla: mide frecuencia de información, no capacidad de supervisión. Se propone abordarla en futuras mediciones con preguntas diseñadas para ese fin.
- **H12 — La concentración en pocos proveedores agravaría el riesgo agregado sin que las organizaciones lo monitoricen.** No es contrastable con este instrumento. El cuestionario mide cómo se gestiona a los terceros, no cómo se distribuye la dependencia entre ellos, que es lo que la hipótesis afirma. El dato adyacente resulta coherente, ya que solo el 8% dispone de planes de salida o sustitución para proveedores críticos, pero no permite pronunciarse sobre la concentración. Es una candidata clara para la siguiente oleada.



6.1.5 Lectura del conjunto

El patrón que emerge de las refutaciones es coherente con el hallazgo central de este informe, y llega a él por una vía independiente. El benchmarking europeo previo esperaba encontrar déficits de naturaleza técnica y operativa: planes de continuidad ausentes, ejercicios de crisis infrecuentes, proveedores sin inventariar. Lo que el dato español muestra es capacidad razonable en todos esos frentes y un freno situado en otro lugar. Las organizaciones españolas sujetas a NIS2 hacen simulacros, tienen planes de continuidad fundamentados e inventarían a sus proveedores. Lo que no hacen es cuantificar el riesgo en términos que el Consejo pueda comparar con los demás riesgos del negocio, ni situar la función de seguridad donde la norma exige.

Las hipótesis que quedan abiertas comparten un rasgo que merece registrarse: en tres de los cuatro casos la limitación no está en los datos sino en el instrumento, que no incluye preguntas sobre la concentración de proveedores, sobre la capacidad efectiva de supervisión del Consejo ni sobre la percepción del propio órgano de gobierno. Son las líneas que un segundo ciclo de medición debería incorporar.

> Las organizaciones españolas muestran madurez operativa; su palanca es integrar la ciberseguridad en las decisiones estratégicas del Consejo. Medir esa brecha exige mejores instrumentos, centrados en gobierno, negocio y proveedores.



ANÁLISIS ECONÓMICO Y DE INVERSIÓN



07

7 ANÁLISIS ECONÓMICO Y DE INVERSIÓN

Esta sección responde a una pregunta que el Consejo formula antes que ninguna otra: cuánto cuesta esto.

La respuesta tiene dos mitades muy desiguales. El coste de cumplir NIS2 lo han estimado cuatro marcos oficiales europeos, con desgloses que en algunos casos llegan al detalle de las horas de personal. El coste de no cumplir no lo ha medido nadie con datos observados: la Comisión Europea solo lo modela y reconoce por escrito que faltan datos, y España no dispone de una estimación oficial del coste económico agregado de los ciberincidentes: las estadísticas públicas (Interior, INCIBE, Banco de España) recogen recuentos de incidentes y delitos, o el fraude en medios de pago, pero no el impacto económico del conjunto. Esa asimetría no es una laguna estadística menor. Determina qué se presupuesta y qué no, y por tanto qué se hace y qué no.

7.1 LO QUE CUESTA CUMPLIR: CINCO MARCOS OFICIALES

Cinco marcos oficiales europeos se han pronunciado sobre el coste de NIS2: cuatro le han puesto precio, con métodos y resultados que no son directamente comparables pero que dibujan un orden de magnitud, y el belga decidió no hacerlo.

La estimación española merece lectura propia, porque es la que afecta a los lectores de este informe. La Memoria del Análisis de Impacto Normativo del anteproyecto cifra en 2.249.696.603 euros el coste de la plena implantación de la norma en el tejido empresarial español, partiendo de un coste medio por entidad de 2.153.250 euros para las esenciales y 179.562 para las importantes, corregido después por un porcentaje de implantación previa del 95%, 48% y 27% según el tipo de entidad. La cifra se presenta de forma agregada, sin desglose por obligación y sin especificar el horizonte temporal al que corresponde. Aplicada a una entidad esencial no regulada previamente, indicaría un coste de 1,12 millones de euros; el Gobierno alemán estima unos 215.000 euros anuales por entidad esencial y el neerlandés unos 100.000 de media. La diferencia puede responder al horizonte temporal considerado, al punto de partida asumido o al perímetro de lo que cada memoria contabiliza. Se recoge aquí como la referencia oficial española disponible sobre el coste de implantación.

Bélgica, uno de los primeros Estados miembros en transponer, no realizó evaluación de impacto: el proyecto declara en su primera página que no se solicitó. Una de las transposiciones más rápidas de Europa se hizo sin calcular lo que costaba.

TABLA 2. Cuatro marcos oficiales han puesto precio a NIS2, con métodos no comparables; solo Alemania y Países Bajos lo desglosan por obligación.

Fuente	Año	Entidades	Coste estimado	Desglose por obligación
Comisión Europea, SWD(2020) 345	2020	~110.000 (UE)	+22% del gasto en seguridad TIC para entidades nuevas; +12% para las ya sujetas a NIS1	No
Alemania, BT-Drs. 21/1501	2025	29.850	2.300 M€/año recurrente +2.200 M€ puntual	Sí, cinco obligaciones
Países Bajos, Cyberbeveiligingsbesluit	2025	8.100	812 M€/año recurrente + 1.348 M€ puntual	Sí, tres obligaciones
España, Memoria del Análisis de Impacto Normativo	2024	5.760 (1.819 esenciales, 3.941 importantes)	2.250 M€ de implantación	No
Bélgica, DOC 55 3862/001	2024	2.400	Sin evaluación de impacto	—

7.2 LO QUE CUESTA NO CUMPLIR

Frente a esa precisión aparente, el otro lado de la balanza está vacío. La Comisión Europea lo dice literalmente en el anexo 1 de su propia evaluación de impacto: no existen datos comparables en la Unión que permitan medir el retorno de la inversión en ciberseguridad. Su única cuantificación, 11.300 millones de euros de daño evitado en diez años, es un modelo lineal construido sobre estimaciones de terceros, y a fecha de hoy no ha sido actualizada.

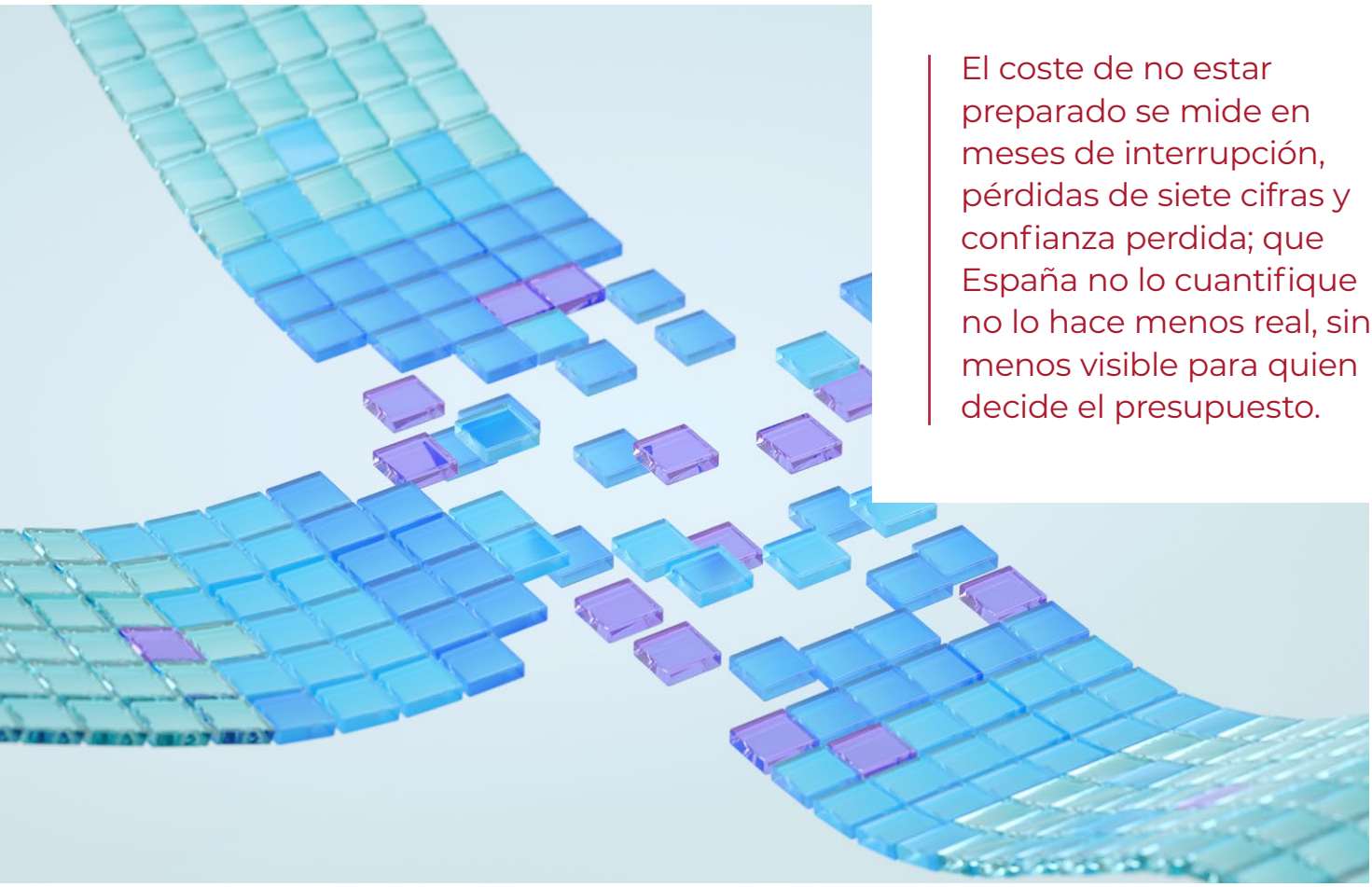
En España no se dispone de una estimación oficial y agregada del coste económico de los ciberincidentes. La información disponible es de actividad: el Informe Anual de Seguridad Nacional agrega cada año los datos de los cuatro equipos de respuesta de referencia, que en 2025 gestionaron 211.478 incidentes en el sector público, 122.223 en ciudadanía, empresas y red académica, y 231 en el ámbito de Defensa, a los que se suman las notificaciones de operadores de servicios esenciales a la Oficina de Coordinación de Ciberseguridad. De los gestionados en el ámbito de ciudadanía y empresas, 401 correspondieron a operadores esenciales e importantes. Son recuentos de actividad de cada equipo, no una medida de incidencia sobre el universo de entidades sujetas.

La única serie española con dimensión monetaria es la del mercado asegurador: Aon estima el volumen de primas de ciberseguro en 190 millones de euros en 2024, un 12% más que el año anterior, con la colaboración de doce aseguradoras y datos que representan en torno al 80% del mercado. Es el precio de transferir el riesgo, no el coste de sufrirlo.

La referencia más sólida disponible es alemana y no es oficial. El estudio *Wirtschaftsschutz 2025* de Bitkom, sobre una encuesta a 1.002 empresas de al menos diez empleados realizada entre abril y junio de 2025, cifra el daño total a la economía alemana en 289.200 millones de euros anuales, de los cuales 202.400 millones se atribuyen a ciberataques. Es una encuesta con extrapolación, no una medición, y procede de una asociación empresarial. Que sea la mejor fuente disponible en Europa para una magnitud de este orden dice más sobre el estado de la evidencia que sobre el estudio.

Conviene ser preciso al comparar estas magnitudes, porque miden cosas distintas: un recuento de incidentes gestionados no es una incidencia poblacional, una encuesta de daño no es una estadística de siniestros, y un modelo de daño evitado no es un coste observado. Ninguna de las tres cifras debe sumarse ni presentarse como equivalente a las otras.





> El coste de no estar preparado se mide en meses de interrupción, pérdidas de siete cifras y confianza perdida; que España no lo cuantifique no lo hace menos real, sino menos visible para quien decide el presupuesto.

Nada de lo anterior debe interpretarse como que el coste de no estar preparado sea pequeño o incierto en su naturaleza. Lo que falta es la medición agregada, no la evidencia del daño, y esa evidencia es consistente en los tres planos que preocupan a un consejo. En el plano operativo, el estudio anual de IBM sobre 600 organizaciones de todo el mundo, con datos de marzo de 2024 a febrero de 2025, encontró que el 86% de las organizaciones sufrió interrupción de sus operaciones tras una brecha y que, de las que se habían recuperado del todo, tres de cada cuatro necesitaron más de cien días. En el plano financiero, el coste medio de una brecha se situó en 4,44 millones de dólares, y en 5,08 millones cuando fue el propio atacante quien reveló la extorsión o el ransomware. En el plano reputacional y de confianza, el propio informe identifica la pérdida de negocio y la atención posterior a los clientes afectados como componentes principales del coste.

El Informe Anual de Seguridad Nacional añade el plano que no se expresa en dinero: para 2025 describe un entorno de amenazas convergentes sobre infraestructuras críticas y señala expresamente el sector del agua, donde se han identificado intrusiones dirigidas a manipular parámetros en sistemas de control industrial.

Conviene precisar el alcance de estas cifras: proceden de una muestra global de conveniencia en la que España no aparece desglosada como país, de modo que sirven para dimensionar el orden de magnitud del daño y su distribución entre planos, no para estimar el coste de un incidente en una organización española. Aun así, permiten afirmar lo esencial: la cuestión no es si protegerse resulta caro, sino que el coste de no hacerlo se materializa en paradas de servicio de meses, en cifras de siete dígitos y en confianza perdida, mientras que ninguna estadística pública española lo agrega. Que no se mida no lo hace menor; lo hace invisible para quien decide el presupuesto.

7.3 EL COSTE REGULATORIO DIRECTO: SANCIONES Y RESPONSABILIDAD PERSONAL

El anteproyecto español establece tres niveles de consecuencia, y el más severo para un consejero no es el económico. Las multas ordinarias alcanzan los 2 millones de euros para infracciones muy graves. El máximo de la Directiva, 10 millones de euros o el 2% de la facturación mundial para entidades esenciales y 7 millones o el 1,4% para importantes, se reserva a dos supuestos concretos: no implantar las medidas exigidas cuando esa omisión haya causado un incidente significativo, y el incumplimiento reiterado de la obligación de notificar.

Por encima de la multa está la responsabilidad personal. El artículo 14 hace al órgano de dirección responsable de aplicar las medidas y de supervisar su implantación efectiva. El artículo 35.2 establece que los miembros del órgano de dirección responden solidariamente de las infracciones que cometa la entidad, sin distinguir entre consejeros ejecutivos y no ejecutivos. El artículo 31.5 permite prohibir temporalmente el ejercicio de funciones de dirección en entidades esenciales, y el artículo 42.4 prevé la publicación de una amonestación en el Boletín Oficial del Estado identificando a la persona responsable. Esa opción española no era la única posible. Países Bajos transpuso el mismo artículo de la Directiva excluyendo expresamente al consejo de supervisión y, cuando los estatutos reparten funciones, a los consejeros no ejecutivos: la obligación recae solo sobre los ejecutivos. Dos Estados miembros, el mismo mandato europeo, alcances personales opuestos.

Todo lo anterior es derecho proyectado, no vigente. El anteproyecto fue aprobado en primera vuelta por el Consejo de Ministros el 14 de enero de 2025 y sometido a audiencia e información pública entre el 16 de enero y el 10 de febrero. Según el Informe Anual de Seguridad Nacional 2025, el Consejo de Estado ha emitido su dictamen y el Ministerio del Interior estudia cómo integrar sus observaciones. El texto no ha superado aún la segunda vuelta en Consejo de Ministros ni ha sido remitido a las Cortes Generales. A la fecha de cierre de este informe, la última versión sometida a audiencia pública sigue siendo la de enero de 2025, y la versión más reciente disponible por cauce oficial es la que España notificó a la Comisión Europea el 21 de febrero de 2025 en el marco de la Directiva (UE) 2015/1535, registrada como notificación 2025/0104/ES.

Las organizaciones españolas se encuentran así ante una asimetría: la expectativa es conocida, la referencia de implementación aún no. El contenido sustantivo de las obligaciones es público desde 2022, y el Reglamento de Ejecución 2024/2690 lo concreta técnicamente, pero solo para los proveedores de infraestructura y servicios digitales. Para el resto de los sectores no existe especificación europea vinculante de qué constituye una medida adecuada y proporcionada, y el principio de proporcionalidad del artículo 21.1 deja esa determinación en manos de la entidad. A ello se añaden otros puntos pendientes de concreción: el registro en el que inscribirse, el criterio de supervisión, y el esquema al que deberá ajustarse la certificación que el anteproyecto exige a las entidades esenciales. La incertidumbre no es solo de plazo, hoy sin fecha, sino sobre todo de estándar de suficiencia.

Esa asimetría no se reparte por igual entre dimensiones. Los requisitos técnicos y operativos disponen de sustrato de referencia: normas internacionales, el Esquema Nacional de Seguridad y, allí donde aplica, el propio Reglamento 2024/2690. La supervisión por el órgano de dirección no dispone de ninguno. El déficit que los datos de este estudio localizan en la integración del riesgo y en la cultura coincide con el punto en el que la cadena regulatoria europea ofrece menos guía de implementación.

> El mayor riesgo no es la multa. Es el daño a la empresa y la responsabilidad personal de sus consejeros, en un marco que todavía no fija qué es suficiente.

7.4 LO QUE NINGÚN SISTEMA PONE EN PRECIO

El hallazgo económico de este estudio no está en ninguna de las cifras anteriores, sino en lo que todas omiten.

Este informe concluye que el factor limitante de la madurez española no es tecnológico: el 77% de las organizaciones ancladas en nivel 2 lo está por su dimensión de gestión de riesgo empresarial o de cultura y capacidades. Dicho de otro modo, lo que falta es capacidad de gobierno. Pues bien, esa capacidad no tiene precio asignado en ningún marco económico europeo.

En el cálculo alemán, el más detallado de Europa, la formación de los miembros del órgano de dirección representa 53,9 millones de euros anuales, en torno al 2,3% del coste recurrente total; la supervisión efectiva del consejo, que el artículo 20 exige, no tiene partida propia y queda absorbida dentro de la gestión de riesgos. En el neerlandés, la línea de gobierno asciende a 120 millones puntuales y 6 millones anuales, y consiste literalmente en formar a seis personas por entidad una vez y a 0,3 al año; la propia memoria explica que las empresas ya formaban a sus consejos internamente y que el coste nuevo surge de exigir formador externo con certificado. En el español no hay partida de gobierno: la única carga administrativa cuantificada del capítulo es la tasa de 97,23 euros por habilitar al responsable de seguridad. En el modelo de la Comisión, ninguna.

El patrón se repite fuera del ámbito regulatorio. Las certificaciones no lo capturan del todo: este estudio muestra que las organizaciones certificadas en ISO 27001 o ENS aventajan a las no certificadas en todas las dimensiones, pero la ventaja es menor precisamente en la integración del riesgo en la gestión empresarial (0,35 puntos), frente a 0,73 en resiliencia operacional. Y el mercado asegurador tampoco: los cuestionarios de suscripción vigentes de las principales aseguradoras se articulan sobre controles técnicos verificables (autenticación multifactor, detección en endpoint, copias inmutables, gestión de parches), e incorporan algún elemento de proceso como el plan de respuesta probado o la gestión de terceros, pero no preguntan por la supervisión del consejo, el reporte al órgano de dirección ni la formación de los administradores. Los brókeres atribuyen la normalización de precios del ciclo 2023-2024 a la implantación obligatoria de esos controles técnicos; no se ha localizado evidencia pública que cuantifique el efecto de la madurez de gobierno sobre la prima, el límite o el deducible.

Conviene subrayar lo que hace especialmente costosa esa omisión: el gobierno es lo único que la evidencia europea disponible asocia de forma directa con mejores resultados. En su estudio de inversiones de 2023, ENISA encontró que las entidades cuyo liderazgo está implicado, entendiendo por tal que recibe formación específica y aprueba formalmente las medidas de gestión de riesgos, tienen más del doble de probabilidad de superar el nivel básico tanto en gestión de riesgos como en detección y respuesta a incidentes, y que la existencia de una política de riesgo de terceros pasa del 36% al 87% cuando el liderazgo aprueba las medidas. España figuraba entonces en el tercer puesto europeo en formación del liderazgo, con un 70%, tras Italia y Alemania. Es decir: la variable que ningún marco económico presupuesta, que ninguna certificación verifica y que ninguna aseguradora pregunta es, a la vez, la que más se asocia con superar el nivel básico de capacidad.

Tres sistemas económicos independientes (el presupuesto regulatorio, la certificación y la transferencia de riesgo) coinciden en medir y poner precio a la capacidad técnica, y en no medir ni poner precio a la capacidad de gobierno.

Mientras tanto, es precisamente la capacidad de gobierno la que la norma exige al Consejo y la que estos datos identifican como el cuello de botella real.

La conclusión no es que gobernar sea barato. Es que no está presupuestado, y lo que no se presupuesta no se ejecuta, no se audita y no se reconoce.

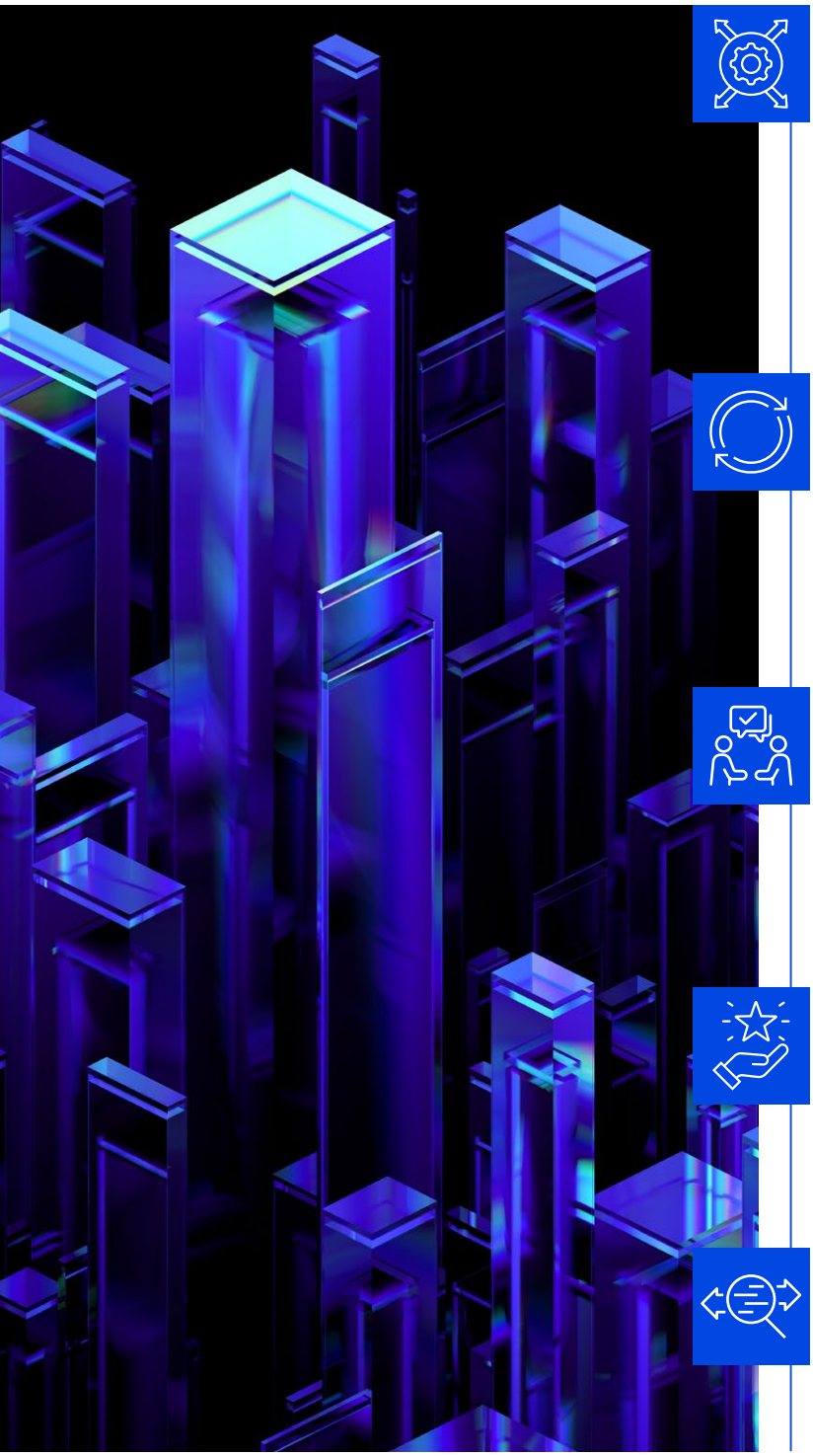
La inversión que permitiría subir de nivel a la mayoría de las organizaciones españolas (integrar el riesgo ciber en el marco de gestión empresarial, dotar de tiempo real la supervisión del Consejo, construir capacidades y cultura) no aparece como línea en ningún cálculo oficial, no se verifica en ninguna auditoría de certificación y no se refleja en ninguna prima. Esa es la brecha que este modelo de madurez se propone hacer visible.

7.5 QUÉ INVERTIR Y CUÁNTO: UNA PROPUESTA

Las secciones anteriores describen un vacío. Esta propone cómo llenarlo. Conviene advertir que lo que sigue es una propuesta razonada a partir de los datos del estudio y de las referencias europeas disponibles, no una estimación validada: ninguna fuente oficial ha calculado el coste de la capacidad de gobierno, y este informe no puede suplir esa ausencia con una cifra propia.

En qué invertir.

Los datos identifican con precisión dónde está el freno. De las organizaciones ancladas en nivel 2, el 77% lo está por gestión de riesgo empresarial o por cultura y capacidades. Las prioridades de inversión que se derivan son cinco, ordenadas por el impacto que tendrían sobre el nivel global:



01/ Integrar el riesgo de ciberseguridad en el marco de gestión de riesgos corporativo, con una metodología de cuantificación documentada que permita expresar la exposición en términos comparables con los demás riesgos del negocio. Es el paso que distingue el nivel 3 del nivel 4 en la dimensión de gestión de riesgo empresarial. Es además la dimensión que con más frecuencia frena a las organizaciones en nivel 2 (§4.2).

02/ Dotar de tiempo y estructura la supervisión del órgano de dirección: un punto recurrente en el orden del día con periodicidad definida, un cuadro de indicadores comprensible para consejeros no técnicos, y constancia documental de las decisiones de aceptación de riesgo. No es inversión en tecnología, es diseño de gobierno.

03/ Formar a los miembros del órgano de dirección con contenido específico sobre identificación de riesgos y evaluación de medidas, impartido por terceros independientes y con constancia de la formación recibida. Es la única partida de gobierno que los marcos europeos han presupuestado, y es la más barata de todas.

04/ Construir capacidades y cultura más allá de la concienciación general: una estrategia explícita de talento que decida qué se desarrolla internamente, qué se contrata y qué se externaliza, y mecanismos de aprendizaje organizativo tras los incidentes.

05/ Extender la gestión de terceros más allá de la contratación, con evaluación continua, criterios de salida y análisis de concentración, que es donde las propias empresas europeas declaran la mayor carga de cumplimiento pendiente.

Cuánto.
La respuesta honesta tiene dos partes. La primera es que una porción de lo que falta ya está tarifada y es modesta: la formación certificada de un miembro del órgano de dirección se estima en 2.469 euros por persona en el cálculo neerlandés. Para un consejo de diez miembros, la obligación formativa del artículo 20 se sitúa en el orden de los veinticinco mil euros iniciales y en torno a mil anuales de mantenimiento. Es una estimación baja porque solo tarifa la formación, no el tiempo de supervisión que el artículo 20 exige al consejo. No es una cifra que decida el presupuesto de ninguna organización sujeta a esta norma.

La segunda parte es la que importa. Según los datos europeos disponibles, las organizaciones destinan una mediana del 9% de su presupuesto de tecnología a ciberseguridad y el 10,6% de su personal de tecnología a funciones de seguridad, y dentro de ese personal la distribución por funciones asigna un 40% a operaciones, un 23% a arquitectura, un 21% a gobierno y riesgo y un 16% a auditoría. En el desglose alemán, cerca de tres cuartas partes del coste de cumplimiento son horas de personal y el resto, costes materiales.

> La conclusión que se desprende es que subir de nivel probablemente no exige más presupuesto, sino reasignación dentro del que ya existe y tiempo del órgano de dirección, que es el recurso que ningún presupuesto refleja.

Dicho en términos operativos para un consejo: la pregunta pertinente no es cuánto más hay que gastar en ciberseguridad, sino qué proporción del gasto actual se dedica a capacidad de gobierno frente a capacidad técnica, con qué frecuencia y durante cuánto tiempo se supervisa el riesgo ciber al máximo nivel, y si esa supervisión deja evidencia. Ninguna de esas tres preguntas requiere una partida nueva para poder responderse, y las tres son las que este modelo de madurez evalúa.

Una recomendación de medición.
Puesto que ningún marco oficial cuantifica la capacidad de gobierno, la propuesta metodológica de este informe es que las organizaciones adopten dos indicadores propios y comparables entre ejercicios: la proporción del presupuesto y del personal de seguridad dedicada a funciones de gobierno y riesgo, y las horas anuales de dedicación efectiva del órgano de dirección a la supervisión de la ciberseguridad. Son magnitudes que cualquier organización puede medir hoy sin coste adicional, y que harían visible precisamente aquello que la contabilidad regulatoria, la certificación y el mercado asegurador dejan fuera.

La inversión en gobierno se amortiza sobre varias normas.
Las organizaciones sujetas a NIS2 no afrontan una norma, sino una secuencia: la propia NIS2 y su transposición, el Reglamento DORA para el sector financiero, la Directiva de resiliencia de entidades críticas, el Reglamento de Inteligencia Artificial, el Reglamento de Ciberresiliencia para productos con elementos digitales y, desde enero de 2026, una propuesta de revisión de la propia NIS2. Cada una exige a los órganos de dirección lo mismo en sustancia: identificar el riesgo, evaluarlo con un método defendible, supervisar las medidas y poder demostrar que lo han hecho.

Esa coincidencia tiene consecuencias sobre cómo conviene invertir. Tanto la capacidad técnica como la de gobierno son necesarias, y ninguna sustituye a la otra: una organización sin controles no protege sus servicios, y una organización sin gobierno no sabe cuáles proteger ni puede demostrar por qué. La cuestión no es elegir entre ambas, sino construir las dos de forma reutilizable, de modo que sirvan para el conjunto de exigencias y no para una norma concreta.

Lo que los datos de este estudio indican es dónde está hoy el margen de mejora. De las organizaciones ancladas en el nivel 2, el 77% lo está por gestión de riesgo empresarial o por cultura y capacidades, y las dimensiones técnicas constituyen el único factor limitante en tres de los treinta y un casos de cuello de botella único. Con ese punto de partida, la hipótesis razonable es que la inversión adicional en capacidad de

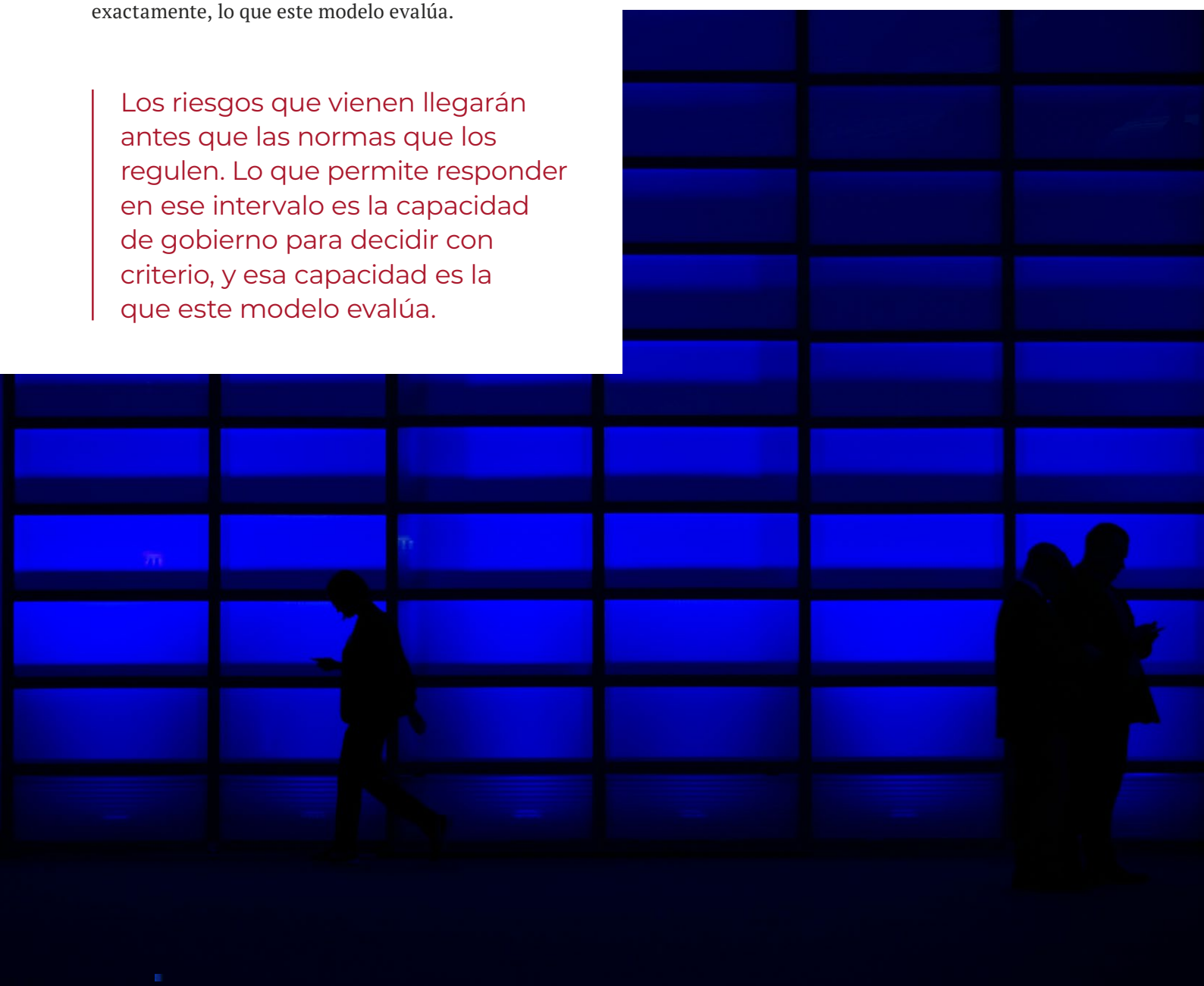
gobierno rinde más que la técnica, y aporta en todo caso algo que esta última no da: flexibilidad ante requisitos que todavía no se conocen.

Y la razón última no es regulatoria. Los riesgos que las organizaciones tendrán que gobernar en los próximos años, desde la dependencia de proveedores tecnológicos hasta la adopción de sistemas de inteligencia artificial en procesos críticos, no llegarán acompañados de un catálogo de controles listo para aplicar. Llegarán antes que las normas que los regulen. Lo que permite responder en ese intervalo no es un control concreto, sino la capacidad de decidir con criterio y con rapidez: identificar el riesgo, evaluarlo, decidir quién asume qué y dejar constancia de esa decisión. Esa capacidad es, exactamente, lo que este modelo evalúa.

> Los riesgos que vienen llegarán antes que las normas que los regulen. Lo que permite responder en ese intervalo es la capacidad de gobierno para decidir con criterio, y esa capacidad es la que este modelo evalúa.

7.6 DATOS PROPIOS: ALCANCE Y LÍMITE

La encuesta no incluyó preguntas sobre el presupuesto de ciberseguridad ni sobre el tamaño del equipo, de modo que este estudio no puede relacionar inversión y madurez ni calcular retornos por nivel. Se recomienda incorporar ambas preguntas en futuras oleadas, junto con una pregunta explícita sobre las horas anuales que el órgano de dirección dedica a supervisar la ciberseguridad, que es hoy la variable ausente en todas las fuentes revisadas.



LECTURA COMPLEMENTARIA Y CONVERGENCIA CUALITATIVA



08

8 LECTURA COMPLEMENTARIA Y CONVERGENCIA CUALITATIVA

8.1 NOTA SOBRE EL ALCANCE DE ESTA SECCIÓN

El cuestionario v2.2 no incluye preguntas abiertas de opinión: es una decisión de diseño para sostener la comparabilidad entre cortes en 15-20 minutos de respuesta. El material disponible se limita a los campos "Otro" de sector (37 respuestas), multisector (31), cargo (31) y certificaciones, de modo que no hay barreras ni experiencias narradas que codificar por dimensión. Lo que sigue no es, por tanto, un análisis temático de la encuesta, sino la lectura de ese texto libre y de las preguntas opcionales del bloque demográfico, que complementan los hallazgos cuantitativos por tres flancos: dónde están las fronteras del ámbito NIS2, quién ocupa realmente la función de seguridad y qué relación hay entre certificarse y gobernar.

El material cualitativo propio del proyecto procede del proceso de validación del modelo y habla de su validez de contenido, no de la radiografía nacional; se recoge en 8.5 como triangulación.

8.2 LAS FRONTERAS DEL ÁMBITO, VISTAS DESDE EL TEXTO LIBRE

37 organizaciones no encontraron su sector en la lista NIS2 y lo escribieron; otras 31 se declaran en más de un sector. Agrupadas por lectura de los Anexos I y II, forman tres grupos: fuera de ámbito con certeza razonable (seguros, con ocho menciones y el grupo más numeroso, medios, hostelería, tercer sector); probablemente en ámbito sin verse en la lista (consultoría de ciberseguridad, proveedores SaaS a sectores críticos, organismos de certificación, defensa, aeronáutica, sanidad pública); y Anexo II no identificado como tal (distribución de alimentos, fabricación, servicios de movilidad).

El caso de los seguros es el más elocuente: ocho aseguradoras respondieron a una encuesta de madurez NIS2 cuando su régimen es DORA, y casi ninguna se declaró fuera del ámbito de la Directiva (Anexo A.9). Esta es la versión cualitativa de la brecha de concienciación de §4.5: el problema no es desconocer la norma, sino que la taxonomía sectorial oficial no coincide con cómo las organizaciones se describen a sí mismas. La implicación para la transposición y para INCIBE es directa: la comunicación del ámbito no puede apoyarse solo en la lista de anexos.

> Muchas organizaciones no se reconocen en la lista de sectores de NIS2: el problema no es desconocer la norma, sino que la clasificación oficial no coincide con cómo se describen a sí mismas.

8.3 QUIÉN RESPONDE: LA FUNCIÓN EXISTE, EL TÍTULO NO SIEMPRE

Solo 85 de 209 respondentes (41%) tienen el título de CISO. 44 son responsables de seguridad sin título C-level y 31 escribieron su cargo, con predominio de perfiles de GRC y de figuras híbridas (SGSI y DPO en la misma persona, CTO con seguridad, resilience manager). La lectura no es solo de muestra: la función de gobierno de la ciberseguridad se está institucionalizando en España por la vía del cumplimiento y del GRC, no por la del C-level.

El cargo declarado y lo que cada respondente contesta sobre el posicionamiento del CISO (P1, línea de reporte, y P3, participación en decisiones estratégicas) son preguntas independientes, de modo que sirven de control mutuo, y la comprobación la pasan: quien se declara sin título C-level sitúa al CISO por debajo de quienes se declaran CISO o CSO. No hay inflación de estatus. Dos matices merecen mención. El primero es que quien más alto sitúa al CISO no es el CISO, sino quien se titula director o responsable de ciberseguridad (el 36% lo sitúa como miembro del comité de dirección o con reporte directo al Consejo, frente al 9% de los CISOs), señal de que el título de dirección se usa donde la función ya está en el comité. El segundo, más relevante, es el CIO con responsabilidad de ciberseguridad: entre las categorías con base suficiente, es la que declara la influencia estratégica más baja, y su D1 media es de 1,95 sobre 5, casi un punto por debajo de la de los CISOs (2,78). Cuando la ciberseguridad cuelga del CIO sin función propia, el gobierno de la seguridad es claramente más débil. Es la lectura empírica de D1.1 y de por qué el modelo insiste en que el acceso y la influencia real importan más que la línea de reporte formal.

> La función de ciberseguridad se institucionaliza por la vía del cumplimiento; cuando depende del CIO, su influencia estratégica es la más baja.

8.4 CERTIFICARSE AYUDA, PERO NO BASTA

Todas las organizaciones respondieron a la pregunta de certificaciones, aunque 18 prefirieron no indicarlas: 87 tienen ISO/IEC 27001, 68 el ENS y 42 ambas; 11 SOC 2, 7 CMMC, y 71 declaran no tener ninguna de las certificaciones propuestas. Entre quienes completaron el modelo, las organizaciones con ISO 27001 o ENS (n=88) tienen un nivel global medio de 2,32 y el 9% alcanza N4 o más; las que no tienen ninguna de las dos (n=70) se quedan en 1,79 y el 3%. La certificación se asocia a más madurez en las cinco dimensiones, pero no lleva a las organizaciones al umbral básico: los certificados siguen, de media, en el nivel 2.

TABLA 3.

La certificación se asocia a más madurez en todas las dimensiones, y menos que en ninguna otra en la integración del riesgo en la gestión empresarial.

Dimensión	Con ISO 27001 o ENS	Sin ninguna de las dos	Diferencia
D3 Resiliencia operacional	3,09	2,36	+0,73
D5 Cultura y capacidades	3,11	2,39	+0,72
D1 Gobierno y liderazgo	2,92	2,25	+0,67
D4 Terceros y cadena de suministro	3,11	2,65	+0,46
D2 Riesgo empresarial	2,71	2,36	+0,35

La menor ventaja aparece precisamente en la dimensión que más frena a las organizaciones según §4.2: la integración del riesgo ciber en la gestión empresarial. Tener ISO 27001 o el ENS se asocia a mejor resiliencia, mejor cultura y mejor gobierno formal, pero predice poco sobre si el riesgo ciber está integrado en el riesgo corporativo. Es lo que el modelo sostiene desde su diseño: el ENS y la ISO/IEC 27001 acreditan que los controles existen, y el modelo evalúa la capacidad de gobierno que los dirige. Los datos muestran que ambas cosas están relacionadas, pero no son lo mismo, y el valor

añadido del diagnóstico de gobierno está precisamente en lo que la certificación no garantiza.

> **Advertencia de interpretación.** La comparación es una asociación descriptiva, no un efecto: la certificación correlaciona con tamaño, sector y recursos, variables que este análisis no controla. Las diferencias de la tabla no deben leerse como lo que una organización ganaría por certificarse.

La consecuencia práctica excede el diagnóstico. La certificación se usa con frecuencia como prueba de preparación ante NIS2, en la relación con clientes, en los pliegos de contratación pública y en la propia conversación con el Consejo. Estos datos marcan su límite: acredita el suelo técnico y dice poco sobre si el riesgo ciber está integrado en el riesgo corporativo o sobre si existe supervisión efectiva del órgano de dirección, que es exactamente lo que el Art. 20 atribuye a la dirección y lo que el Art. 21.1 exige evaluar de forma proporcionada. Una certificación vigente y una supervisión inexistente son compatibles: una de cada diez organizaciones certificadas declara que su Consejo no recibe ningún informe regular de ciberseguridad. Para el regulador, la implicación es que la certificación no debería tratarse como proxy de preparación; para el Consejo, que un certificado vigente no es una respuesta a la pregunta de si la organización está gobernando su riesgo ciber.

8.5 CONVERGENCIA CON EL PANEL DE VALIDACIÓN

El componente cualitativo procede del proceso de validación del modelo, en dos talleres y una sesión individual con trece expertos, CISOs y responsables de riesgo de grandes organizaciones españolas de los sectores de energía, infraestructuras, industria, tecnología, telecomunicaciones, transporte, banca, hostelería y salud. Doce de ellos completaron la valoración de validez de contenido, con un S-CVI/Ave global de 0,917, y el proceso arrojó nueve patrones temáticos. Su valor aquí es de triangulación: los patrones cualitativos explican y convergen con los hallazgos cuantitativos.

El freno es de gobierno, no de tecnología, también en la voz de los expertos.
Dos patrones lo sostienen. El primero, que la mera existencia de documentos (planes, políticas, certificados) no equivale a resiliencia real, que es lo que muestra 8.4 con los datos de certificación. El segundo, que la sofisticación técnica no sustituye a una gobernanza sólida. Ambos convergen con el hallazgo central de la encuesta: la meseta del nivel 2 se explica sobre todo por la integración del riesgo en la gestión empresarial y por la cultura, no por las dimensiones técnicas.

La distinción declarada/percibida/validada estaba anticipada. Uno de los patrones del panel introdujo explícitamente la diferencia entre madurez declarada, percibida y validada con evidencias. Es el fundamento conceptual del análisis de §4.4: el modelo mide capacidad de gobierno, no autopercepción, y por eso la autopercepción y la medición divergen de forma distinta según la regla de agregación. Este estudio mide la madurez descrita por el responsable de seguridad; la validada con evidencias queda para la aplicación del modelo en cada organización (§1.2).

El posicionamiento del CISO como cuestión recurrente. El panel insistió en que el posicionamiento real del CISO (acceso e influencia, no línea de reporte formal) es determinante, lo que motivó la reformulación de la dimensión de gobierno en el modelo v2.0. El dato de 8.3 sobre el CIO con responsabilidad de ciberseguridad le da soporte empírico.

Calibración y observabilidad. Los patrones más citados (proporcionalidad del salto N3→N4 y necesidad de una guía de evidencias observables) son de naturaleza metodológica y se incorporaron al modelo v2.0. El único descriptor que quedó en alerta en el CVI, D4.2 (evaluación de terceros, I-CVI 0,67), se reformuló hacia efectividad y continuidad, admitiendo certificaciones como evidencia válida.

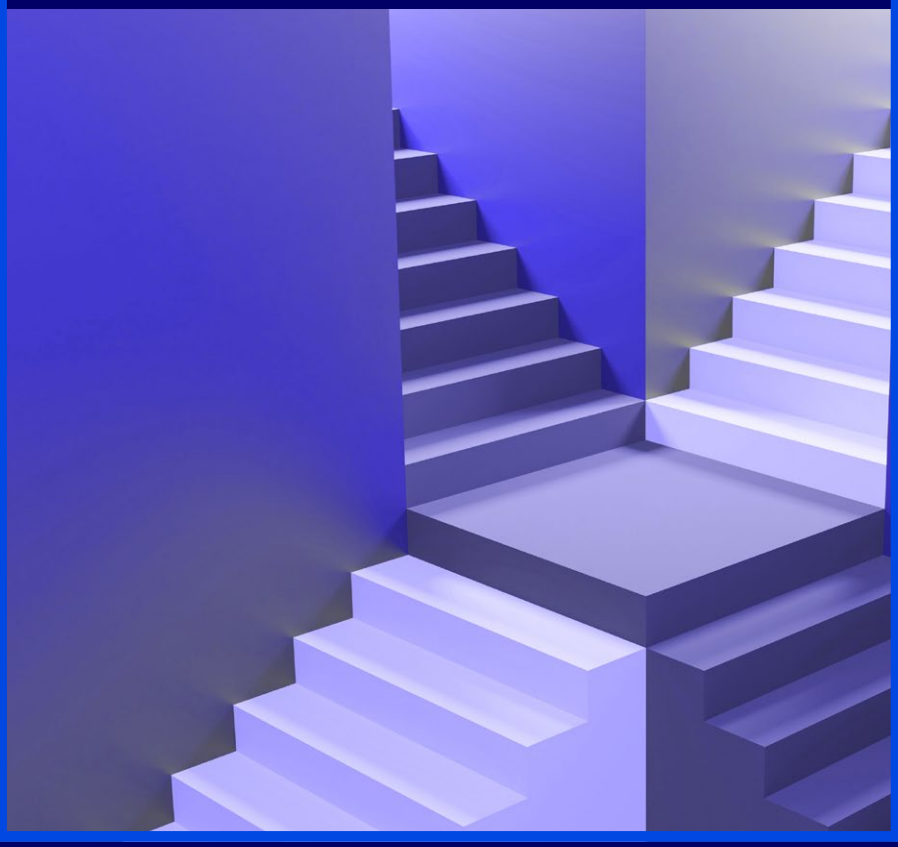


8.6 LA AMBICIÓN A 24 MESES

Las preguntas opcionales de nivel objetivo y nivel alcanzable a 24 meses dibujan la distancia entre dónde están las organizaciones y dónde quieren estar (n=166). El 64% se fija como objetivo el nivel 4 o superior; hoy lo alcanza el 7%. El salto medio entre el nivel actual y el objetivo declarado es de 1,6 niveles, y el 57% se propone subir dos niveles o más. Entre las entidades esenciales el contraste es máximo: el 93% aspira a N4 o más y el 12% está ahí; entre las importantes, el 44% aspira a un nivel por encima de su propio umbral. El 84% considera que su objetivo es alcanzable.

La pregunta sobre el principal estímulo para avanzar, de respuesta múltiple y disponible para 165 respondentes, reparte las motivaciones: el 43% señala el cumplimiento obligatorio, y 54 organizaciones lo citan sin mencionar convencimiento previo alguno, mientras que el 41% afirma que el convencimiento de mejorar ya existía y que NIS2 solo ha puesto fechas. La exigencia de clientes o socios sujetos a NIS2 aparece en el 25% (el efecto cadena de suministro ya opera como palanca) y un incidente propio o sectorial en el 14%. Conviene leer la opción de convencimiento previo con la cautela de la deseabilidad social; aun así, la lectura es que la obligación regulatoria y la presión de la cadena mueven tanto o más que la convicción interna, y eso encaja con el resto del cuadro. Puesta junto a los hallazgos anteriores, la conclusión es la del informe entero: una comunidad ambiciosa, que sabe dónde quiere estar en dos años, pero que se propone un salto grande desde una capacidad anclada en gobierno y cultura. Subir de nivel no es un proyecto de controles, es una decisión de presupuesto y de agenda del Consejo, y que el 93% de las esenciales aspire a N4 mientras lo alcanza el 12% es la cifra que debería abrir esa conversación.

CONCLUSIONES Y RECOMENDACIONES



09

9 CONCLUSIONES Y RECOMENDACIONES

Siete conclusiones ordenan el diagnóstico:

01 **Siete de cada diez organizaciones no alcanzan el umbral de cumplimiento básico.** El 72% se queda por debajo del nivel 3 y solo el 7% alcanza el nivel 4, que corresponde al cumplimiento robusto. La meseta está en el nivel 2, por debajo del umbral, no en él.

02 **Lo que frena no es la tecnología, es el gobierno:** integrar el riesgo ciber en la gestión empresarial y en la cultura corporativa. El 77% de las organizaciones ancladas en el nivel 2 lo está por riesgo empresarial o por cultura y capacidades; las dimensiones técnicas son el único freno en tres de los treinta y un casos de cuello único. La validación experta lo confirma.

03 **Existe una brecha de concienciación sobre el propio alcance de la norma.** El 30% no se identifica con certeza como sujeto a NIS2, y de las 24 organizaciones que afirman que no les aplica, 15 sí están en su ámbito y 11 son entidades esenciales.

04 **Los responsables de seguridad se valoran por su media, no por su dimensión menos madura.** Dos de cada tres se sitúan por encima del nivel que les asigna el modelo, pero su autopercepción casi coincide con la media de sus cinco dimensiones (+0,2). La distancia procede sobre todo de la regla: el modelo exige que todas las dimensiones estén a la altura, y basta una para fijar el nivel.

05 **La fotografía real es probablemente menos madura que la muestra**, por el sesgo de cobertura hacia organizaciones que ya tienen función de seguridad (§4.6).

06 **Certificarse ayuda, pero no basta.** Las organizaciones con ISO/IEC 27001 o ENS puntúan más alto en las cinco dimensiones, pero siguen de media en el nivel 2, y su menor ventaja está precisamente en la integración del riesgo en la gestión empresarial (+0,35, frente a +0,73 en resiliencia operacional). La certificación acredita los controles; la capacidad de gobierno que los dirige requiere un trabajo propio (§8.4).

07 **La capacidad que falta no es específica de NIS2.** El déficit identificado es de gobierno del riesgo tecnológico, no de cumplimiento de una norma concreta. Las organizaciones analizadas afrontan simultáneamente NIS2, la resiliencia de entidades críticas, el reglamento de inteligencia artificial, el de ciberresiliencia de productos y, en el sector financiero, DORA, además de una propuesta de revisión de la propia NIS2 presentada en enero de 2026. Todas ellas reclaman del órgano de dirección la misma capacidad: evaluar un riesgo tecnológico con método, supervisarlo con evidencia y responder de esa supervisión. Una organización que resuelva ese mecanismo para el riesgo ciber dispondrá del andamiaje para los demás; una que afronte cada norma como un proyecto separado acumulará marcos de cumplimiento sin construir capacidad. El diagnóstico de este informe, por tanto, no describe únicamente el estado de preparación ante NIS2: describe la capacidad disponible para gobernar el riesgo tecnológico en general.

Dónde actuar: las prácticas que más fallan.

Las conclusiones anteriores se leen por dimensión. El cuestionario permite bajar un nivel más: cada pregunta describe una práctica observable, y se puede contar cuántas organizaciones están por debajo de la práctica que corresponde al nivel 3. Ninguna práctica sale bien parada: en las once, entre un tercio y dos tercios de las organizaciones se sitúan por debajo. Tres destacan con claridad sobre el resto:

- **Cuantificar el riesgo en términos económicos.** Es la práctica más débil del estudio: el 64% no pone cifra económica a su riesgo ciber, y solo el 14% lo cuantifica de forma sistemática. La proporción es prácticamente igual en entidades esenciales (62%) que en importantes (64%).
- **Dar al responsable de seguridad acceso a la dirección.** En el 56% de las organizaciones reporta a un responsable técnico o a un directivo funcional, o no existe; solo una de cada cuatro le da acceso regular al comité de dirección o al Consejo.
- **Integrar el riesgo ciber en la gestión de riesgos corporativa.** El 51% lo gestiona al margen del marco corporativo, mientras que el 41% lo tiene plenamente integrado. Es la práctica más polarizada: casi no hay término medio.

Las otras ocho prácticas se sitúan entre el 35% y el 48% y no admiten un orden fiable con esta muestra. Las mejor resueltas, en términos relativos, son las técnicas y documentales: el inventario de terceros críticos, el análisis de impacto que sustenta la continuidad y los ejercicios de crisis. Es el mismo patrón del informe, observado ahora práctica a práctica. De ahí se derivan dos acciones concretas por dimensión, que corresponden a los pasos hacia los niveles 3 y 4 del modelo (tabla 4).

Dos cautelas. Son prácticas declaradas por el responsable de seguridad, no verificadas con evidencias. Y las diferencias entre sectores solo son relevantes en unos pocos casos, que se recogen en el Anexo A: la cuantificación en las administraciones públicas, la evaluación de terceros y la cultura en manufactura, la línea de reporte del responsable de seguridad en alimentación y el caso de la banca, con la madurez técnica consolidada y el salto pendiente en el gobierno.

TABLA 4. Qué práctica falla en cada dimensión y qué acción concreta acerca al nivel 3 y al 4.

Dimensión	Qué falla (organizaciones por debajo del nivel 3)	Acción concreta
Gobierno y liderazgo	El 43% informa al Consejo como mucho una vez al año, dentro de los informes de tecnología; en una de cada cuatro, el Consejo no recibe información regular o solo la recibe tras un incidente. Solo el 25% de los responsables de seguridad participa en la mayoría de las decisiones estratégicas.	Informe trimestral de ciberseguridad con punto propio en la agenda del Consejo. Participación del responsable de seguridad en la definición del apetito de riesgo y en la planificación anual.
Gestión de riesgo empresarial	El 64% no estima su riesgo en términos económicos. El 51% lo gestiona al margen del marco corporativo.	Rangos económicos para los principales escenarios, sin necesidad de metodologías complejas. Misma metodología que el resto de riesgos e inclusión en el mapa de riesgos corporativo.
Resiliencia operacional	El 41% no hace ejercicios de crisis periódicos; solo el 36% los hace con la alta dirección. El 37% no tiene un análisis de impacto que sustente sus planes de continuidad.	Un ejercicio de mesa anual con la alta dirección. Planes de continuidad basados en un análisis de impacto y probados al menos una vez al año.
Gestión de terceros	El 48% no evalúa a sus proveedores o solo lo hace al contratarlos. El 35% no los clasifica por criticidad.	Evaluación anual de la seguridad de los proveedores críticos y, como paso siguiente, cláusulas contractuales y derecho de auditoría. Inventario de proveedores clasificado por criticidad y revisado cada año.
Cultura y capacidades	El 43% se limita, como mucho, a una formación básica anual sin diferenciar por rol. El 41% no pasa de recordatorios periódicos.	Formación por rol con simulaciones y métricas de seguimiento. Campañas regulares en las que participe toda la organización.

Recomendaciones por destinatario.

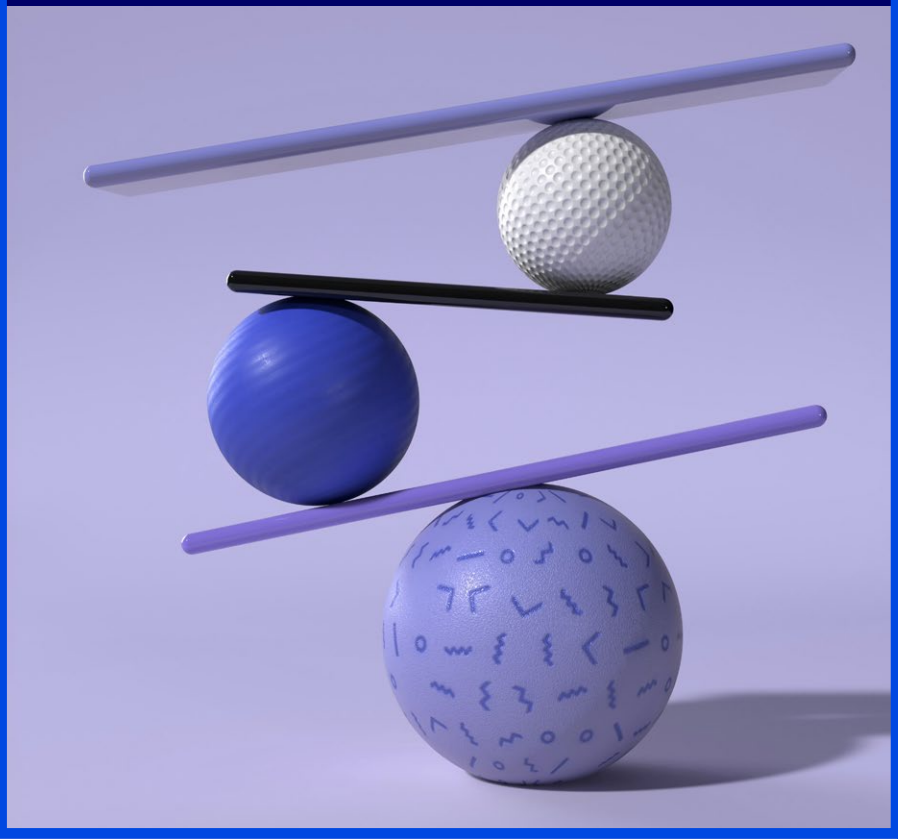
Para el equipo directivo, y en particular para el CISO.
Si la organización está en N2, el retorno marginal no está en más tecnología, sino en integrar el riesgo ciber en la gestión empresarial (D2) y en la cultura y las capacidades de la organización (D5). Ninguna de las dos palancas pertenece a la función de seguridad: la primera corresponde al marco corporativo de gestión de riesgos y la segunda a la política de personas, de modo que la decisión es del comité de dirección.

Para el Consejo.
NIS2 le hace responsable de aprobar y supervisar las medidas (Art. 20), y la barrera detectada es de gobierno, justo su terreno indelegable. La evidencia de que el Consejo fue informado, deliberó y decidió no es solo una exigencia de cumplimiento: es el presupuesto de la diligencia que ampara al propio consejero. El estándar exigible es el de apply and explain (King IV): no basta declarar adhesión, hay que poder explicar cómo se aplica y qué resultado produce.

Para el regulador.
El esfuerzo de comunicación de INCIBE y de las autoridades competentes debería priorizar la identificación de entidades sujetas y el alcance a los sectores y organizaciones hoy fuera del radar (agua, investigación, entidades pequeñas), no solo la difusión de requisitos. Conviene además no tratar la certificación como indicador de preparación NIS2: acredita el suelo técnico, no la capacidad de gobierno que el Art. 20 atribuye a la dirección.



LIMITACIONES Y CAUTELAS METODOLÓGICAS



10

10 | LIMITACIONES Y CAUTELAS METODOLÓGICAS

Momento de la medición:
las cifras corresponden al cierre de la encuesta en septiembre de 2026 y describen una situación previa a la entrada en vigor de la transposición española.

Regla del mínimo:
el nivel global se concentra en N2 en parte por diseño de la regla, que toma la dimensión menos madura. Todo enunciado de nivel se hace bajo la regla del modelo y se acompaña de la distribución por media de dimensiones (§10.1).

Autopercepción frente al modelo:
los responsables de seguridad se sitúan por encima del modelo frente a la regla del mínimo (+0,8) y casi coinciden con él frente a la media de sus dimensiones (+0,2). La distancia procede sobre todo de la regla de agregación (§4.4).

Concordancia en importantes (58%):
menor que en esenciales (92%); 19 organizaciones que se declaran importantes son objetivamente esenciales. Parte de la diferencia puede deberse a los límites del clasificador objetivo descritos en §3.3, que trabaja con bandas de tamaño.

Casos sin nivel global:
40 respuestas no tienen nivel global por dimensiones no contestadas; siete de ellas, del panel experto, por diseño (ver 10.2).

Excepciones de entidad (DNS, TLD, servicios de confianza):
no son distinguibles con los datos de la encuesta y quedan fuera del alcance de este análisis.

10.1 TRAZABILIDAD DE LOS TAMAÑOS DE MUESTRA (N)

Los distintos tamaños de muestra que aparecen en el informe no son errores: responden a un embudo de compleción y a una asimetría de regla que conviene dejar trazada.

El embudo. La encuesta se responde en orden y los ítems de madurez van al final, con D5 la última, de modo que el n cae a medida que avanza el cuestionario. Sobre 209 respondentes totales, los ítems de cada dimensión los completan 193 (D1), 185 (D2), 180 (D3), 178 (D4) y 169 (D5); de ahí los n variables de la tabla de medias por dimensión (§4.1). Solo 169 respondentes completan las cinco dimensiones, que es el requisito de la regla del mínimo, y por eso 169 es el n del nivel global y del análisis del cuello de botella (§4.2). De esos, 166 contestaron además la autopercepción (Q24), que es el n del gap frente a la regla del mínimo (§4.4).

La cascada es limpia:
- 209 entran
- 169 completan las cinco dimensiones
- 166 se autoevalúan además.

La asimetría de regla: dos vistas de la regla de la media. La regla del mínimo exige las cinco dimensiones y se calcula, por tanto, sobre 169 respuestas. La regla de la media admite dos lecturas y el informe presenta ambas. La **vista restringida** se calcula sobre los mismos 169 perfiles completos y es la directamente comparable con la regla del mínimo: arroja una media de 2,73 y un 18% de organizaciones en nivel 4 o superior. La **vista ampliada** aprovecha toda la información disponible y se calcula sobre las 192 respuestas que completaron al menos una dimensión: arroja una media de 2,79 y un 20% en nivel 4 o superior.

La diferencia entre ambas tiene una causa identificable. Los 23 respondentes que entran en la vista ampliada y no en la restringida comparten un rasgo: a todos les falta la dimensión de cultura y capacidades, a ocho de ellos por diseño (panel experto, que respondió la versión anterior de esa pregunta) y al resto por abandono. Sus puntuaciones en las dimensiones que sí contestaron son más altas que las de los perfiles completos (3,06 frente a 2,71). La vista ampliada es, en consecuencia, ligeramente optimista, y así debe interpretarse.

La magnitud del efecto es reducida: 2 puntos porcentuales en la proporción que alcanza el nivel 4 y 0,06 en la media, sin alteración de la forma de la distribución. Se reportan las dos porque ninguna es superior a la otra en términos absolutos: la restringida garantiza la comparabilidad entre reglas, la ampliada aprovecha el máximo de información recogida. El contraste entre autopercepción y modelo no se ve afectado, ya que solo cuatro de esos 23 respondentes contestaron la pregunta de autoevaluación.

Alcance del objeto medido:
el instrumento evalúa la capacidad de gobierno del riesgo de ciberseguridad tomando NIS2 como marco de referencia. No mide la gobernanza de otros riesgos tecnológicos, en particular la relativa al uso de inteligencia artificial, que plantea cuestiones propias de supervisión, responsabilidad y competencia del órgano de dirección. La conclusión sobre la transferibilidad de la capacidad de gobierno se apoya en la coincidencia sustantiva de lo que las distintas normas exigen a los órganos de dirección, no en una medición directa; contrastarla empíricamente exigiría un instrumento que evaluase ambas gobernanzas sobre la misma muestra, lo que constituye una línea natural de extensión de este trabajo.

10.2 RESPUESTAS INCOMPLETAS Y POSIBLE SESGO DE NO RESPUESTA

40 de las 209 respuestas no permiten calcular el nivel global porque falta al menos una dimensión. Conviene examinar si esas ausencias son aleatorias, porque de no serlo afectarían a la interpretación de los resultados.

Hay que separar dos causas. Ocho de las respuestas incompletas proceden del panel experto, y en siete de ellas la ausencia no es abandono: respondieron la versión anterior de la pregunta de cultura, que no se puntúa con la escala actual. Del resto, 23 proceden del canal ISMS Forum. Las ausencias crecen de forma monótona con la posición de la dimensión en el cuestionario, de 16 en D1 a 40 en D5, un patrón característico del abandono progresivo y no de la evitación de preguntas concretas, lo que apunta a la extensión del instrumento como causa principal.

La dimensión con más ausencias, cultura y capacidades organizacionales, es también una de las dos que sostienen el segundo hallazgo de este informe, de modo que conviene acotar el efecto. Los datos apuntan a que las respuestas incompletas corresponden, si acaso, a organizaciones algo más maduras: puntúan más alto en las dimensiones que sí contestaron (§10.1). En el supuesto más favorable, que la dimensión ausente no fuera la menos madura de ninguna de ellas, incluirlas situaría la proporción por debajo del nivel 3 en el 68% en lugar del 72%. El primer hallazgo, siete de cada diez organizaciones por debajo del cumplimiento básico, se mantiene en cualquier caso.

Se recomienda, en futuras oleadas, registrar el punto de abandono y reducir la extensión del bloque final.

REFERENCIAS

NORMATIVA

Directiva (UE) 2022/2555, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (NIS2).

Reglamento de Ejecución (UE) 2024/2690, sobre requisitos técnicos y metodológicos de las medidas de gestión de riesgos y especificación de incidentes significativos.

Reglamento (UE) 2022/2554, sobre resiliencia operativa digital del sector financiero (DORA).

Reglamento (UE) 2024/2847, sobre requisitos horizontales de ciberseguridad para los productos con elementos digitales (Reglamento de Ciberresiliencia).

Reglamento Delegado (UE) 2024/1366, por el que se establece un código de red sobre normas sectoriales para los aspectos de ciberseguridad de los flujos transfronterizos de electricidad.

Directiva (UE) 2022/2557, relativa a la resiliencia de las entidades críticas.

Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad.

Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad, Ministerio del Interior, trámite de audiencia e información pública de 16 de enero de 2025, y su Memoria del Análisis de Impacto Normativo, noviembre de 2024; texto notificado a la Comisión Europea el 21 de febrero de 2025 en el marco de la Directiva (UE) 2015/1535, notificación 2025/0104/ES, Sistema de Información sobre Reglamentaciones Técnicas (TRIS).

ESTUDIOS Y FUENTES SECTORIALES

Aon España (2025). *VI Estudio sobre Ciberseguridad y Gestión del Riesgo Ciber en España*.

Bitkom (2025). *Wirtschaftsschutz 2025*.

Cisco (2025). *Cybersecurity Readiness Index 2025*.

CyberSmart (2026). *NIS2 Research 2026*.

Deloitte (2024). *Global Future of Cyber Survey*, 4.ª edición.

EY Center for Board Matters (2025). *Cyber and AI oversight disclosures: what companies shared in 2025*.

Financial Stability Board (2026). *Sound Practices for Responsible Adoption of Artificial Intelligence, informe sometido a consulta*.

Financial Stability Board (2023). *Enhancing Third-Party Risk Management and Oversight: a toolkit for financial institutions and financial authorities*.

Hiscox (2024). *Informe de Ciberpreparación*.

Howden (2024). *Cyber Report*.

IBM Security y Ponemon Institute (2025). *Cost of a Data Breach Report 2025*.

IDC y Microsoft (2026). *Preparing for NIS2 and Beyond*.

Marsh. *Elevated Cyber Risk*.

Proofpoint (2025). *Voice of the CISO,* corte España.

World Economic Forum (2025). *Global Cybersecurity Outlook 2025*.

FUENTES OFICIALES EUROPEAS Y NACIONALES

Comisión Europea (2020). *Impact Assessment accompanying the proposal for a Directive on measures for a high common level of cybersecurity across the Union*, SWD(2020) 345.

ENISA (2026). *NIS360 2026*.

ENISA (2025). *NIS Investments 2025*.

ENISA (2025). *NIS360 2024*.

ENISA (2023). *NIS Investments 2023*.

ENISA (2023). *Demand Side of Cyber Insurance in the EU*.

Departamento de Seguridad Nacional (2026). *Informe Anual de Seguridad Nacional 2025*.

Departamento de Seguridad Nacional (2025). *Informe Anual de Seguridad Nacional 2024*.

INCIBE (2026). *Balance de Ciberseguridad 2025*.

Bundesamt für Sicherheit in der Informationstechnik (2026). *NIS-2 in Zahlen*, actualizado a 30 de junio de 2026.

Deutscher Bundestag (2025). *Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie*, Drucksache 21/1501, y *Beschlussempfehlung und Bericht des Innenausschusses*, Drucksache 21/2782.

Tweede Kamer der Staten-Generaal (2025). *Cyberbeveiligingswet, Memorie van Toelichting*, Kamerstuk 36 764, nr. 3, y *Nota van toelichting bij het Cyberbeveiligingsbesluit*.

Chambre des représentants de Belgique (2024). *Projet de loi établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique,* DOC 55 3862/001 y 3862/002.

MARCO CONCEPTUAL Y METODOLÓGICO

Copeland, T. y Antikarov, V. (2001). *Real Options: A Practitioner's Guide*.

Freeman, R.E. (1984). *Strategic Management: A Stakeholder Approach*.

Hollnagel, E. (2006). *Resilience Engineering: Concepts and Precepts*.

Institute of Directors in South Africa (2016). *King IV Report on Corporate Governance for South Africa*.

Lynn, M.R. (1986). *Determination and quantification of content validity*. Nursing Research, 35(6).

O'Reilly, C.A. y Tushman, M.L. (2004). *The ambidextrous organization*. Harvard Business Review.

Polit, D.F. y Beck, C.T. (2006). The content validity index: are you sure you know what's being reported? *Research in Nursing & Health,* 29(5).

Schoemaker, P.J.H. (2002). *Profiting from Uncertainty*.

Wack, P. (1985). Scenarios: uncharted waters ahead. *Harvard Business Review*.

Woods, D.D. (2015). Four concepts for resilience and the implications for the future of resilience engineering. *Reliability Engineering & System Safety,* 141.

ANEXO A | Perfiles sectoriales

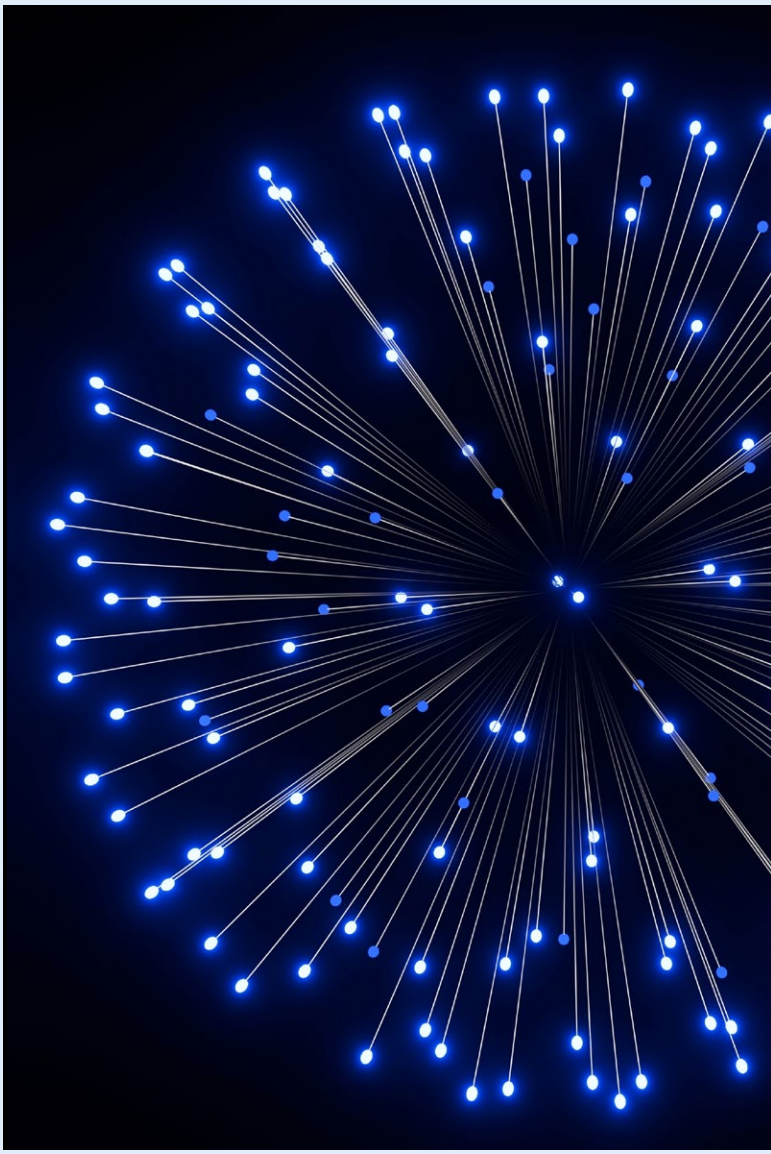
NOTA METODOLÓGICA

Tienen capítulo propio los sectores con al menos quince respuestas: Banca y Finanzas, Infraestructura Digital y TIC, Transporte, Energía, Sanidad, Administraciones Públicas, Manufactura y Alimentación. El resto se agrupa en *Demás* sectores. La media de cada sector se calcula sobre las organizaciones que responden a las cinco dimensiones, y la de cada dimensión sobre todas las respuestas disponibles en ella, por lo que las cinco medias dimensionales no tienen por qué promediar exactamente la media del sector. La media de referencia de los ocho sectores con perfil propio es 2,74 sobre 5.

Los sectores se presentan en las mismas tres bandas de la sección 4.3, no en un orden: banda alta (Banca y Finanzas, Infraestructura Digital y TIC, Transporte), banda media (Energía, Sanidad) y banda baja (Manufactura, Administraciones Públicas, Alimentación). Las bases sectoriales oscilan entre quince y veintisiete respuestas. Son suficientes para describir tendencias y agrupar sectores en bandas, pero no para establecer diferencias finas: las distancias inferiores a dos décimas no deben interpretarse como jerarquía.

Por razones de protección de los participantes, este anexo no publica desgloses por tamaño de organización ni recuentos de entidades esenciales e importantes dentro de cada sector; se describe en su lugar el perfil dominante en términos cualitativos. Tampoco publica la proporción de organizaciones en nivel 4 o superior por sector: en ningún sector superan las dos, de modo que una sola respuesta movería la cifra entre cinco y ocho puntos. Se publica en su lugar la proporción que no alcanza el nivel 3, calculada sobre las organizaciones con nivel global calculable, entre trece y veintiuna por sector.

Lectura transversal. En los ocho sectores, la dimensión que con más frecuencia fija el nivel global de sus organizaciones es el gobierno y liderazgo, la gestión de riesgo empresarial o la cultura y capacidades. En ninguno lo son la resiliencia operacional ni la gestión de terceros. El hallazgo central del informe se reproduce sector a sector.





A.1 BANCA Y FINANZAS

Perfil en los datos.
Banda alta. Media 3,15 sobre 5 (n=24), la más alta de los ocho sectores, a quince centésimas de Infraestructura Digital. Fortaleza en gestión de terceros (3,61, el valor más alto registrado por cualquier sector en cualquier dimensión); debilidad relativa en gobierno y liderazgo (2,89). El 60% no alcanza el nivel 3. Perfil de entidades mixto entre esenciales e importantes

Lectura del sector.
Banca está en la banda alta por la vía esperable: es el sector español con más tradición de supervisión prudencial en materia operativa, y eso se nota en la gestión de terceros. Su 3,61 no procede de NIS2 sino de la acumulación de exigencias previas sobre externalización y, más recientemente, de DORA. El dato revelador no es su posición, sino dónde flaquea: su dimensión más baja es el gobierno y liderazgo, aunque en ella siga por encima de casi todos los demás sectores, y lo que con más frecuencia fija el nivel global de sus organizaciones es el gobierno o la cultura. Un sector que ha industrializado el control de proveedores no ha llevado con la misma intensidad la ciberseguridad al órgano de dirección. El contraste se ve también práctica a práctica: solo el 9% de sus organizaciones está por debajo del nivel 3 en análisis de impacto para la continuidad y en inventario de terceros críticos, pero el 68% no estima su riesgo ciber en términos económicos y en el 59% el responsable de seguridad no reporta por encima de un directivo técnico o funcional. Con la madurez técnica ya consolidada, el salto que le queda es el de gobierno.

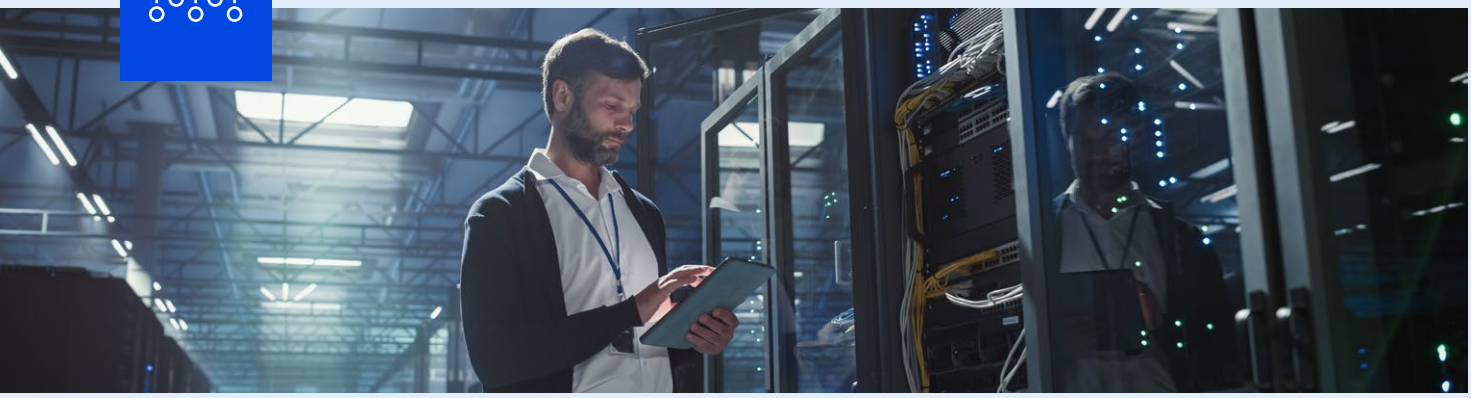
Comparación con otros sectores.
Su ventaja sobre Infraestructura Digital es de quince centésimas, una distancia que las bases muestrales no permiten considerar significativa. La diferencia real aparece al mirar dentro: Infraestructura Digital lidera en gobierno; Banca, en terceros y en resiliencia. Son perfiles de madurez distintos, no grados del mismo perfil. Frente a la banda baja, la distancia es de unos dos tercios de punto, y se concentra en terceros (un punto) y en resiliencia operacional (más de ocho décimas), no en gobierno (tres décimas).

Diferenciación europea.
La evaluación sectorial de ENISA sitúa a la banca, junto con la electricidad y las telecomunicaciones, en la banda de alta madurez y alta criticidad, posición que mantiene desde la primera edición. En 2026 se incorporaron a esa banda las infraestructuras de mercados financieros, impulsadas por la aplicación de DORA. ENISA observa, no obstante, que la implicación directiva es mayor en los bancos de mayor tamaño y que constituye un área de mejora en el resto de entidades financieras, un matiz coherente con el perfil español, donde la fortaleza del sector se concentra en la gestión de terceros y su dimensión más baja es el gobierno.

Recomendaciones y regulación conectada.
El marco conectado es DORA, que para las entidades financieras desplaza el régimen de gestión de riesgos y notificación de NIS2, y la supervisión del Banco de España y la CNMV. DORA prevalece sobre NIS2 en gestión de riesgos y notificación, pero no saca a las entidades de crédito del ámbito de la Directiva; que casi un tercio de las entidades del sector declare que NIS2 no les aplica sugiere que esa frontera tampoco está clara. El margen de mejora del sector no está en controles ni en terceros, sino en el gobierno y la cultura, que son las dimensiones que con más frecuencia limitan su nivel global: la implicación efectiva del órgano de dirección y el aprendizaje organizativo tras incidentes. A ello se suma la cuantificación económica del riesgo, que dos de cada tres entidades del sector no hacen. Para las más avanzadas, el salto siguiente exige gobernanza prospectiva: escenarios, opciones estratégicas y capacidad de anticipación, no más control.

Conclusión del sector.
Banca demuestra que una supervisión sostenida produce madurez técnica y contractual duradera. Su siguiente salto está en llevar esa misma disciplina al gobierno y a la cultura de las organizaciones.

A.2 INFRAESTRUCTURA DIGITAL / TIC



Perfil en los datos.
Banda alta. Media 3,00 sobre 5 (n=27, la base sectorial más amplia). Fortalezas en cultura y capacidades (3,21) y en resiliencia operacional (3,18); debilidad en gestión de riesgo empresarial (2,50). El 63% no alcanza el nivel 3. Perfil predominantemente de entidades esenciales.

Lectura del sector.
Es el sector que lidera en gobierno y liderazgo (3,09), lo que refleja una característica estructural: en las organizaciones cuyo negocio es la tecnología, la seguridad no compite por la atención del comité de dirección, forma parte de la conversación de producto. Su resiliencia operacional es la segunda más alta, consecuencia de operar servicios con compromisos de disponibilidad contractuales. La brecha está en la integración con la gestión de riesgo empresarial: 2,50, casi siete décimas por debajo de su propia resiliencia, y la dimensión que fija el nivel global en cuatro de cada cinco de sus organizaciones. Sabe sostener el servicio; su palanca es traducir ese riesgo al lenguaje del riesgo corporativo.

Comparación con otros sectores.
Comparte la banda alta con Banca y Transporte. Con Banca, por razones opuestas: Banca destaca en terceros por presión supervisora; Infraestructura Digital, en gobierno y resiliencia por la naturaleza del negocio. Es además un sector heterogéneo, que agrupa realidades muy distintas, desde operadores de telecomunicaciones hasta proveedores de servicios gestionados.

Diferenciación europea.
ENISA sitúa las telecomunicaciones y los servicios de confianza en la banda de alta madurez, mientras que los subsectores digitales por defecto, esto es, servicios centrales de internet, nube y centros de datos, se mantienen en la parte alta de la banda moderada. El dato europeo converge de forma notable con el perfil español: ENISA observa que cerca de la mitad de los proveedores de nube y centros de datos declara que los riesgos identificados solo se registran, sin priorizarse ni tratarse de forma sistemática. Es la misma carencia que muestran los datos españoles en la dimensión de gestión de riesgo empresarial, medida con un instrumento distinto.

Recomendaciones y regulación conectada.
Marco conectado: el Reglamento de Ejecución 2024/2690, que fija requisitos técnicos y metodológicos específicos para proveedores de DNS, servicios en la nube, centros de datos, redes de distribución de contenidos, servicios gestionados y de confianza, y que es directamente aplicable sin necesidad de transposición. Es el único subsector con especificación técnica vinculante ya en vigor en el marco de NIS2. La recomendación prioritaria es cerrar la brecha de gestión de riesgo empresarial: cuantificar el riesgo en términos comparables con el resto del negocio y llevarlo al mismo cuadro de mando que los demás riesgos corporativos.

Conclusión del sector.
Es el sector con mejor gobierno de la ciberseguridad y con la mayor distancia entre esa fortaleza y la integración del riesgo en la gestión empresarial. Sabe proteger su servicio; su palanca es expresarlo como riesgo de negocio.

A.3 TRANSPORTE



Perfil en los datos.

Banda alta. Media 2,84 sobre 5 (n=18). Fortaleza en gestión de terceros (3,17); debilidad en gobierno y liderazgo (2,52). El 67% no alcanza el nivel 3. Predominio de entidades esenciales.

Lectura del sector.

En gobierno, Transporte está en el extremo opuesto a Infraestructura Digital: alto en terceros, bajo en gobierno. Es coherente con un sector donde la cadena de suministro es el elemento operativo central y donde la seguridad se ha construido históricamente desde la operación, no desde la dirección. Su gobierno, con 2,52, queda por debajo de la media de los ocho sectores y es la dimensión que con más frecuencia fija el nivel global de sus organizaciones. Resulta especialmente relevante porque predominan las entidades esenciales, para las que el cumplimiento robusto exige nivel 4. Es también el sector con mayor dispersión interna: su media agrupa organizaciones muy distantes entre sí.

Comparación con otros sectores.

Comparte con Energía el patrón de los sectores de infraestructura física: madurez operativa y de cadena de suministro por encima de la madurez de gobierno.

Diferenciación europea.

La evaluación europea distingue con claridad entre modos de transporte. La aviación ascendió en 2026 a la banda de alta madurez, mientras que el ferrocarril y el transporte marítimo permanecen en la zona de riesgo, es decir, con una criticidad superior a su madurez. ENISA señala además que dos de cada cinco empresas del sector continúan excluyendo la tecnología operacional de sus evaluaciones de ciberseguridad, lo que ayuda a explicar por qué la preparación operativa avanza de forma desigual pese a la madurez del sector en la gestión de terceros.

Recomendaciones y regulación conectada.

Marco conectado: la Directiva CER sobre resiliencia de entidades críticas, cuya transposición en España sigue una vía legislativa propia, separada de la de NIS2, y la normativa sectorial aeronáutica, ferroviaria y marítima. La prioridad para el sector es llevar la ciberseguridad al órgano de dirección con la misma formalidad con que ya gestiona la seguridad física y operacional, ámbito en el que el sector tiene una cultura consolidada. El modelo de gobierno ya existe; el paso pendiente es extenderlo al riesgo digital.

Conclusión del sector.

Transporte gestiona bien lo que puede tocar. Su palanca de mejora es aplicar al riesgo digital la cultura de seguridad operacional que ya tiene consolidada.

A.4 ENERGÍA



Perfil en los datos.
Banda media. Media 2,76 sobre 5 (n=16). Cultura y capacidades, gestión de terceros y resiliencia operacional prácticamente igualadas (entre 2,90 y 2,97); debilidad en gobierno y liderazgo (2,47). El 53% no alcanza el nivel 3. Predominio claro de entidades esenciales.

Lectura del sector.
Energía presenta la paradoja más interesante del anexo: casi la mitad de sus organizaciones alcanza el nivel 3 o superior, una de las proporciones más altas del estudio, y al mismo tiempo su gobierno es de los más bajos y fija el nivel global en casi nueve de cada diez de ellas. La explicación está en la distribución interna: junto a esa mitad, un tercio de sus organizaciones está en el nivel inicial. Conviven organizaciones con décadas de regulación de seguridad de suministro con otras que acceden por primera vez a un régimen de ciberseguridad formal. El sector no es homogéneo, y su media oculta esa polarización.

Comparación con otros sectores.
Su perfil dimensional se parece al de Transporte, con la madurez operativa por encima de la de gobierno. La diferencia es la forma de la distribución: Transporte concentra a la mayoría de sus organizaciones en el nivel 2; Energía se reparte entre el nivel inicial y el nivel 3.

Diferenciación europea.
ENISA identifica la energía como sector de máxima criticidad y sitúa la electricidad en la banda de alta madurez, con el gas mejorando y el petróleo por detrás. Un dato europeo contrasta con el perfil español: ENISA observa que la mayoría de las entidades del subsector eléctrico declara cualificaciones formales en ciberseguridad a nivel directivo y formación regular a la dirección, mientras que en esta muestra la energía presenta una de las puntuaciones más bajas en gobierno y liderazgo. La divergencia puede deberse a la composición de la muestra española, que agrupa subsectores con niveles de regulación muy distintos. El Informe Anual de Seguridad Nacional sitúa además la energía entre los sectores estratégicos más expuestos de 2025.

Recomendaciones y regulación conectada.
Marco conectado: la Directiva CER, el código de red europeo de ciberseguridad para los flujos transfronterizos de electricidad (Reglamento Delegado (UE) 2024/1366) y la supervisión de la CNMC. Para el sector, la palanca es el gobierno: llevar el riesgo ciber al Consejo con métricas comparables a las de seguridad de suministro, que el sector ya domina. La madurez técnica existe; lo que falta es su traducción al lenguaje de la dirección.

Conclusión del sector.
Un sector con capacidad operativa contrastada y con la palanca de mejora a su alcance: aplicar al riesgo ciber la disciplina de gobierno que ya ejerce sobre la seguridad de suministro.

A.5 SANIDAD



Perfil en los datos.

Banda media. Media 2,69 sobre 5 (n=21). Fortaleza en gestión de riesgo empresarial (2,82), caso singular entre los ocho sectores; debilidad en gobierno y liderazgo (2,41), seguida de cultura y capacidades (2,47). El 76% no alcanza el nivel 3. Predominio de entidades esenciales.

Lectura del sector.

Sanidad es el único sector cuya dimensión más fuerte es la gestión de riesgo empresarial, lo que probablemente refleja una cultura de gestión del riesgo clínico y de protección de datos de salud trasladada al ámbito digital. Su problema está en el gobierno y en la cultura, ambas entre las más bajas de los ocho sectores, y en que tres de cada cuatro organizaciones no alcanzan el nivel 3 en un ámbito donde predominan las entidades esenciales, para las que el cumplimiento robusto exige nivel 4. El patrón se repite práctica a práctica: Sanidad está por encima de la media de fallo en nueve de las once prácticas evaluadas, y la excepción más clara es precisamente la integración del riesgo ciber en la gestión de riesgos corporativa.

El estudio no diferenció entre sanidad pública y privada, de modo que ambas están reflejadas en este perfil sin que sea posible separarlas. La distinción no es trivial, porque no coincide con la línea del marco regulatorio: hay entidades de titularidad privada sujetas al Esquema Nacional de Seguridad. Convendrá incorporar esa diferenciación en futuras oleadas de la encuesta.

Comparación con otros sectores.

Es uno de los sectores donde más pesa la distancia entre su criticidad social y su posición en la medición. Comparte con las Administraciones Públicas el carácter de servicio esencial a la ciudadanía, pero con el patrón invertido: mejor integración del riesgo y peor gobierno.

Diferenciación europea.

ENISA mantiene la sanidad en la zona de riesgo, con madurez moderada y criticidad superior a ella, y atribuye el progreso observado al mejor desempeño de las entidades farmacéuticas y a la atención política recibida por hospitales y proveedores asistenciales. Entre las carencias que identifica figuran las restricciones de recursos, los niveles bajos de higiene cibernética y la preparación ante incidentes, que coinciden con la cultura y las capacidades, una de las dos dimensiones más débiles del perfil español.

Recomendaciones y regulación conectada.

Marco conectado: el Esquema Nacional de Seguridad en la sanidad pública, el Reglamento General de Protección de Datos por el tratamiento de datos de salud, y el Reglamento de productos sanitarios en lo relativo a dispositivos conectados. La prioridad es la capacidad y la cultura: formación específica por rol asistencial, y capacidad de gestión de incidentes que contemple la continuidad de la atención, no solo la recuperación de sistemas.

Conclusión del sector.

Sanidad sabe gestionar riesgo, porque lleva décadas haciéndolo en el ámbito clínico. Su palanca es llevar esa experiencia al gobierno del riesgo digital y sostenerla con capacidad organizativa.

A.6 ADMINISTRACIONES PÚBLICAS



Perfil en los datos.

Banda baja. Media 2,49 sobre 5 (n=23). Fortaleza en gobierno y liderazgo (2,71); debilidad en gestión de riesgo empresarial (2,17), uno de los valores más bajos del estudio. El 76% no alcanza el nivel 3. Predominio de entidades esenciales.

Lectura del sector.

El perfil de las administraciones públicas es el que mejor se explica por su marco normativo. El sector se sitúa por debajo de la media en cuatro de las cinco dimensiones, y la única que se mantiene en ella es el gobierno y liderazgo, que es precisamente lo que el Esquema Nacional de Seguridad formaliza: política de seguridad, responsable designado y marco organizativo documentado. Su mayor distancia respecto del resto está en la gestión de riesgo empresarial, que el ENS no exige en términos de negocio, porque una administración no dispone de un marco de riesgo corporativo comparable al de una empresa. El resultado es un sector con la estructura de gobierno formalizada por norma y el riesgo sin integrar. La práctica que más lo muestra es la cuantificación: el 86% de las administraciones no estima su riesgo ciber en términos económicos, frente al 64% del conjunto, lo que dificulta priorizar la inversión en seguridad frente a otras necesidades del servicio.

Comparación con otros sectores.

Es el caso más nítido del hallazgo central del informe: el marco de control está formalizado por norma, y el paso pendiente es la capacidad de gobierno que lo orienta a resultados. Su distancia con el resto de sectores sujetos a NIS2 es de en torno a medio punto en gestión de riesgo empresarial y en resiliencia operacional, y de casi cuatro décimas en cultura y capacidades, mientras que en gobierno y liderazgo no hay diferencia apreciable.

Diferenciación europea.

ENISA sitúa la administración pública en la zona de riesgo, con una madurez baja-moderada que describe como fase temprana, y la identifica como el sector más atacado de la Unión. Observa además que la administración pública europea figura entre los sectores con menor implicación y competencia directiva, con en torno a un tercio de las entidades sin un enfoque estructurado para asegurar competencia en ciberseguridad a nivel directivo y cerca de la mitad sin formación para su dirección. La muestra española no reproduce ese rasgo con la misma intensidad: el gobierno y liderazgo del sector se sitúa en la media de los sectores sujetos a NIS2, y el posicionamiento formal del responsable de seguridad queda algo por encima de ella, lo que resulta coherente con una exigencia que el Esquema Nacional de Seguridad impone con carácter obligatorio y que pocos Estados miembros aplican con un esquema equivalente. La supervisión efectiva por el órgano de dirección, en cambio, no se distingue de la del resto de sectores. El perfil resultante es consistente con lo observado en la sección 8.4: el marco formaliza la figura y la estructura, y la capacidad de gobierno que debe dirigirlas es el paso siguiente.

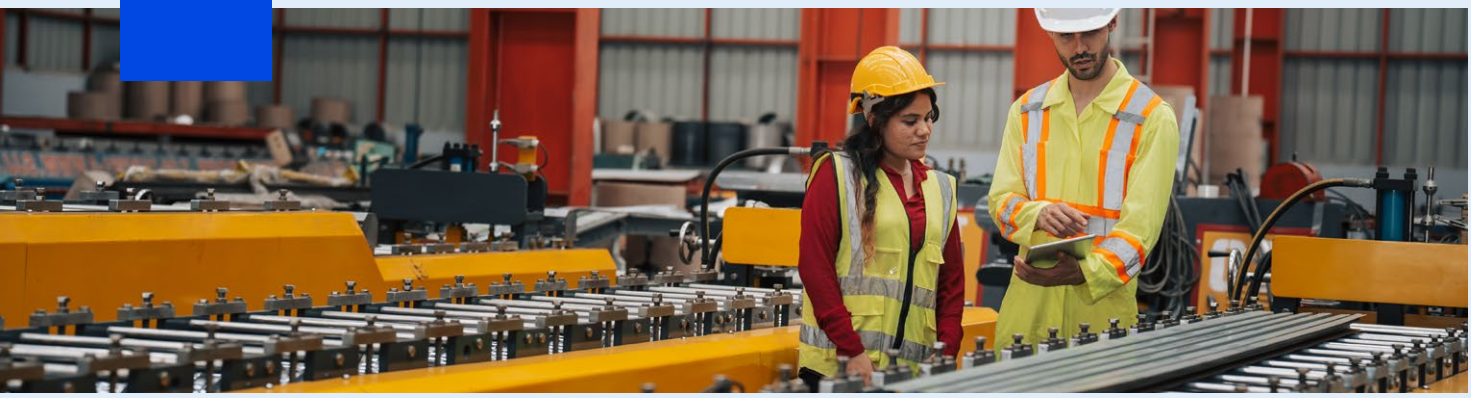
Recomendaciones y regulación conectada.

Marco conectado: el Esquema Nacional de Seguridad, obligatorio, con su sistema de evaluación INES, y los esquemas de interoperabilidad. La prioridad es construir un equivalente funcional de la gestión de riesgo empresarial, adaptado a la lógica de servicio público: qué servicios son críticos para el ciudadano, qué impacto tendría su interrupción, expresado en términos económicos o de servicio comparables, y cómo se decide la aceptación de ese riesgo al nivel adecuado. La administración local, con menos recursos, requiere además mecanismos de apoyo compartido.

Conclusión del sector.

Las administraciones públicas parten de la estructura de gobierno más formalizada por norma de todo el estudio. Su palanca de mejora es apoyarse en ella para integrar el riesgo, tomando como referencia los servicios prestados y su impacto sobre la ciudadanía.

A.7 MANUFACTURA



Perfil en los datos.

Banda baja. Media 2,57 sobre 5 (n=20). Fortaleza relativa en resiliencia operacional (2,62) y en gobierno y liderazgo (2,58); debilidad en gestión de riesgo empresarial (2,21). Más del 90% de las organizaciones con nivel global calculable no alcanza el nivel 3. Predominio de entidades importantes.

Lectura del sector.

Manufactura es, con Alimentación, el sector con más organizaciones por debajo del nivel 3. Al tratarse sobre todo de entidades importantes, para las que el nivel 3 es el cumplimiento básico, casi todo el sector queda hoy por debajo de ese umbral. Su fortaleza relativa en resiliencia refleja una cultura de continuidad de producción anterior a cualquier norma de ciberseguridad: una planta parada es un coste inmediato y visible, y eso ha generado capacidad de recuperación. Pero se trata de continuidad industrial, no necesariamente de continuidad frente a incidentes de origen digital. Sus puntuaciones en gestión de terceros (2,47) y en cultura y capacidades (2,42) están entre las más bajas del estudio, y la distancia se concentra en dos prácticas: el 73% no evalúa a sus proveedores o solo lo hace al contratarlos, frente al 48% del conjunto, y el 69% no pasa de recordatorios periódicos en materia de cultura, frente al 41%.

Comparación con otros sectores.

Comparte con Alimentación el perfil de sector compuesto sobre todo por entidades importantes, con umbral de cumplimiento en nivel 3, lo que puede explicar en parte una menor presión percibida. La diferencia con la banda alta no está en un componente concreto sino en todos a la vez: es una distancia estructural, no una carencia puntual.

Diferenciación europea.

No se dispone de comparación europea para este sector. La evaluación sectorial de ENISA cubre únicamente los sectores de alta criticidad del Anexo I de NIS2, y la manufactura pertenece al Anexo II, que agrupa a los sectores críticos incorporados por la Directiva sin historia previa de regulación de ciberseguridad.

Recomendaciones y regulación conectada.

Marco conectado: la norma IEC 62443 para sistemas de control industrial, y el Reglamento de Ciberresiliencia para productos con elementos digitales, en vigor desde diciembre de 2024, con obligaciones de notificación de vulnerabilidades e incidentes desde septiembre de 2026 y plena aplicación en diciembre de 2027. La prioridad es básica y por eso alcanzable: identificar, clasificar y evaluar periódicamente los terceros críticos, pasar de los recordatorios a campañas regulares en las que participe toda la organización, extender la continuidad existente a escenarios de origen ciber, y establecer un reporte regular al órgano de dirección donde hoy no existe. Para un sector mayoritariamente de entidades importantes, alcanzar el nivel 3 de forma consistente ya supone cumplimiento.

Conclusión del sector.

Manufactura sabe recuperar la producción. Su palanca es aplicar esa misma lógica de continuidad al riesgo digital y a su cadena de suministro. El punto de partida es bajo y, por eso mismo, las primeras mejoras son las que más se notan.

A.8 ALIMENTACIÓN



Perfil en los datos.

Banda baja. Media 2,48 sobre 5 (n=15, la base sectorial más reducida y por tanto la de lectura más prudente). Fortaleza relativa en cultura y capacidades (2,73) y en gestión de terceros (2,58); debilidad en resiliencia operacional (2,27) y en gobierno y liderazgo (2,33), las dos entre las más bajas del estudio. Más del 90% de las organizaciones con nivel global calculable no alcanza el nivel 3. Predominio de entidades importantes.

Lectura del sector.

Alimentación comparte la banda baja con Manufactura y las Administraciones Públicas, a apenas unas centésimas, y esa distancia no debe leerse como jerarquía. Su fortaleza relativa en terceros es probablemente un efecto de la trazabilidad alimentaria, que ha obligado al sector a conocer y controlar su cadena de suministro con un detalle poco común, aunque por razones de seguridad alimentaria y no de ciberseguridad. Su debilidad en resiliencia operacional es, en cambio, llamativa en un sector donde la continuidad del suministro tiene consecuencias directas sobre la población. Su gobierno tiene una expresión concreta: en el 79% de sus organizaciones el responsable de seguridad reporta a un responsable técnico o a un directivo funcional, o no existe, frente al 56% del conjunto.

Comparación con otros sectores.

Comparte con Manufactura ser el sector donde casi ninguna organización alcanza el nivel 3. La diferencia está en el perfil: Manufactura se apoya en la continuidad de producción; Alimentación, en la trazabilidad y en una cultura organizativa algo más sólida, y es precisamente en continuidad donde muestra su mayor carencia.

Diferenciación europea.

Como en el caso de la manufactura, no existe comparación europea disponible: el sector pertenece al Anexo II de NIS2 y queda fuera del alcance de la evaluación sectorial de ENISA, que cubre los sectores de alta criticidad del Anexo I.

Recomendaciones y regulación conectada.

Marco conectado: la normativa de trazabilidad y seguridad alimentaria, y parcialmente la Directiva CER para los operadores de mayor tamaño. La prioridad es la continuidad operacional frente a incidentes digitales, dado el impacto directo del sector sobre el abastecimiento, y llevar ese riesgo al órgano de dirección, empezando por dar al responsable de seguridad acceso directo a ella. La disciplina de trazabilidad que el sector ya domina es la palanca: si sabe reconstruir el recorrido de un lote, puede inventariar y clasificar sus dependencias tecnológicas.

Conclusión del sector.

Alimentación dispone de una cultura de trazabilidad poco común en otros sectores. Su palanca es transferirla a la gestión de su cadena de suministro digital y a la continuidad frente a incidentes de origen ciber.

A.9 DEMÁS SECTORES



Perfil en los datos.

Cuarenta y cinco respuestas no alcanzan el umbral de quince necesario para tener capítulo propio y se agrupan aquí. Dos tercios proceden de organizaciones cuyo sector no figura entre los de NIS2, entre ellas las del sector asegurador; el resto se reparte entre el sector del agua, la investigación y otros sectores de los anexos de la Directiva, con bases muestrales de entre dos y ocho respuestas. Ninguna de esas bases permite publicar medias sectoriales con garantías, de modo que este apartado describe sin cuantificar.

Agua.

Es el sector con base más amplia de este grupo y el que mayor atención merece. ENISA mantiene el agua potable y las aguas residuales entre los sectores menos maduros de todo su análisis, dentro de la zona de riesgo, con un enfoque de gestión del riesgo que califica de reactivo y ad hoc y con dificultades añadidas por la heterogeneidad de operadores, las restricciones de recursos y la prevalencia de sistemas heredados. El Informe Anual de Seguridad Nacional lo sitúa entre los sectores estratégicos más expuestos de 2025 y documenta intrusiones dirigidas a manipular parámetros en sistemas de control industrial. La combinación de criticidad alta, madurez baja y base muestral reducida aconseja tratarlo como área de atención prioritaria más que como resultado medido.

Seguros.

Ocho organizaciones del sector asegurador respondieron a la encuesta. El seguro no figura entre los sectores de NIS2: las entidades aseguradoras están sujetas al Reglamento DORA, con exigencias sobre el órgano de dirección equivalentes en sustancia a las del artículo 20. Sin embargo, casi ninguna se declaró fuera del ámbito de la Directiva: la mayoría se consideró sujeta o probablemente sujeta, o no supo responder. Es la otra cara de la brecha documentada en la sección 4.5: allí, organizaciones sujetas que no lo saben; aquí, organizaciones reguladas por otro instrumento que se creen sujetas. No están menos reguladas, sino reguladas de otra forma. Su presencia en la muestra confirma además que el interés por autoevaluar la madurez de gobierno no se limita a las entidades formalmente sujetas a la Directiva.

Investigación y otros sectores del anexo.

Las bases muestrales son demasiado reducidas para describir un perfil. Su presencia en la muestra es, sin embargo, informativa: se trata de sectores incorporados por NIS2 sin regulación previa de ciberseguridad, en los que la brecha de conocimiento sobre el propio ámbito de aplicación documentada en este informe resulta más probable.

Organizaciones de sectores no incluidos en NIS2.

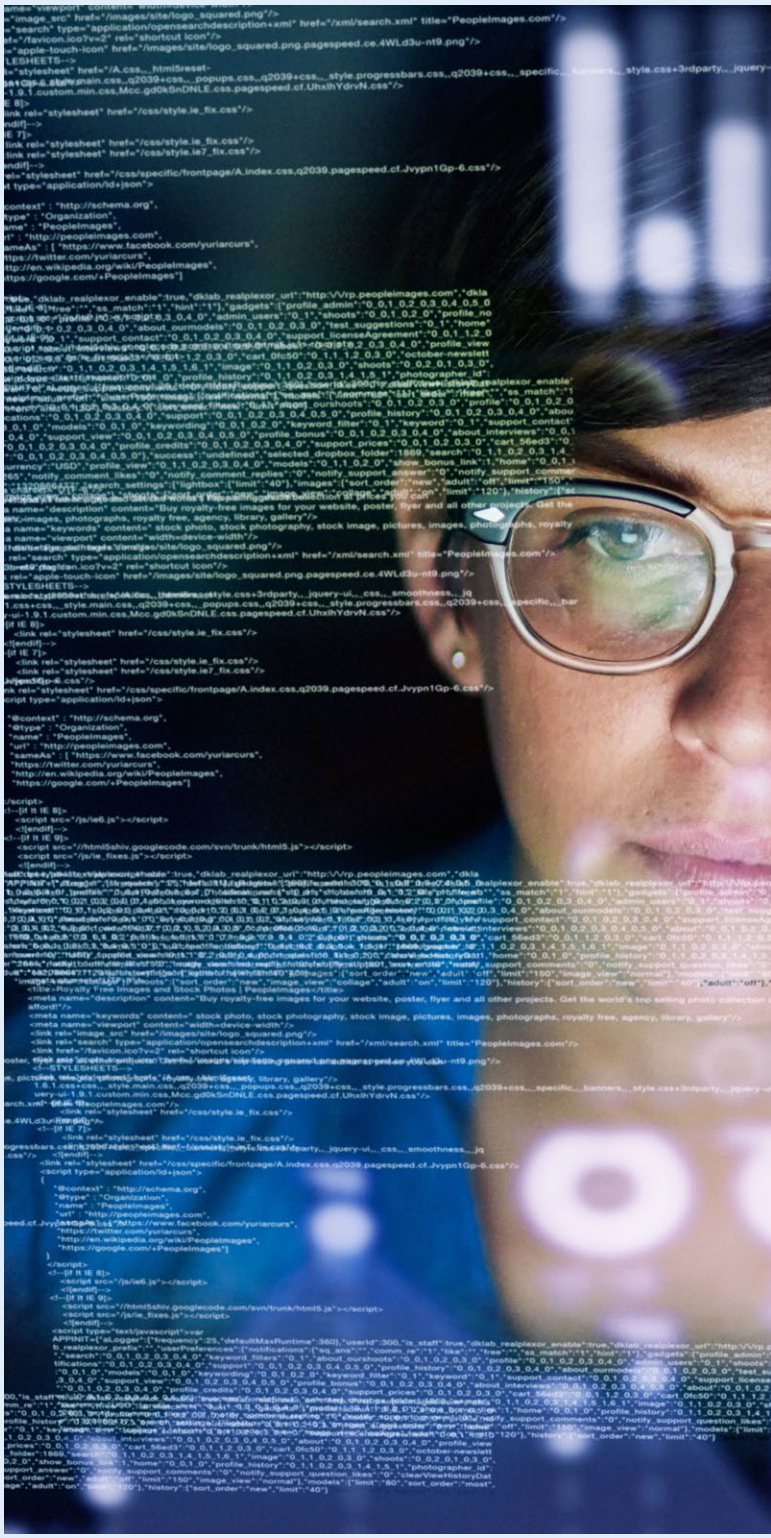
Treinta respuestas, entre ellas siete de las ocho aseguradoras, proceden de organizaciones que eligieron un sector no incluido en los anexos de la Directiva. Se han conservado en el conjunto de datos porque el análisis de aplicabilidad de la sección 4.5 contrasta la clasificación declarada con la derivada objetivamente. No se ha construido un perfil sectorial con ellas.

FUENTES DEL ANEXO

La sección *Perfil* en los datos de cada sector procede del conjunto de datos del estudio (n=209). Los apartados de Diferenciación europea se apoyan en las siguientes fuentes externas:

- **ENISA (2026).** *NIS360 2026.* Agencia de la Unión Europea para la Ciberseguridad, mayo de 2026. Tercera edición. Evalúa madurez y criticidad de los sectores de alta criticidad del Anexo I de NIS2 mediante un índice compuesto que integra legislación, preparación de las entidades, capacidad de las autoridades nacionales y estructuras del ecosistema. Es la fuente de las bandas sectoriales y de las observaciones sobre implicación directiva, tratamiento del riesgo en proveedores de nube y centros de datos, exclusión de tecnología operacional en transporte y posición de los subsectores energéticos.
- **ENISA (2025).** *NIS360 2024.* Primera edición, publicada en febrero de 2025. Se utiliza para contrastar la evolución de las bandas sectoriales entre ediciones.
- **Departamento de Seguridad Nacional (2026).** *Informe Anual de Seguridad Nacional 2025.* Fuente de las observaciones sobre sectores estratégicos más expuestos y sobre incidentes en sistemas de control industrial del sector del agua.
- **Reglamento (UE) 2022/2554 (DORA).** Marco de referencia para las entidades financieras y aseguradoras citadas en A.9.
- **Reglamento de Ejecución (UE) 2024/2690.** Requisitos técnicos y metodológicos aplicables a proveedores de servicios digitales, citado en A.2.
- **Reglamento Delegado (UE) 2024/1366.** Código de red sobre ciberseguridad de los flujos transfronterizos de electricidad, citado en A.4.
- **Reglamento (UE) 2024/2847** (Reglamento de Ciberresiliencia). Requisitos de ciberseguridad para productos con elementos digitales, citado en A.7.
- **Real Decreto 311/2022,** por el que se regula el Esquema Nacional de Seguridad. Marco de referencia de A.6.

Los sectores de Manufactura y Alimentación pertenecen al Anexo II de NIS2 y quedan fuera del alcance de la evaluación sectorial de ENISA, por lo que sus apartados de diferenciación europea señalan expresamente la ausencia de comparación disponible.



ANEXO B | Hipótesis de trabajo del benchmarking internacional

Hipótesis formuladas antes de la medición, con la dimensión del modelo a la que se refieren, la pregunta prevista para su contraste, la referencia externa de la que proceden y el veredicto obtenido sobre esta muestra.

#	Dimensión	Hipótesis	Contraste	Referencia externa	Veredicto
H1	General	Madurez media entre N2 y N3, con predominio de N2 en entidades importantes	Nivel global	—	Confirmada
H2	D1	La mayoría de responsables de seguridad reporta a un directivo funcional o técnico, no al primer ejecutivo	Q13	Deloitte	Confirmada
H3	D1	La alineación entre responsable de seguridad y Consejo está entre las más bajas del entorno	Q14	Proofpoint España 2025	No contrastable
H4	D2	La cuantificación formal del riesgo será escasa; predominio de la evaluación cualitativa	Q17	Foro Económico Mundial	Confirmada
H5	D1	Menor participación del responsable de seguridad en decisiones estratégicas en entidades importantes	Q15	—	Confirmada
H6	D3	Continuidad de negocio y objetivos de recuperación ex ante como área de déficit	Q19	ENISA	Refutada
H7	D3	Baja frecuencia de ejercicios de crisis	Q18	—	Refutada
H8	D4	Inventario de terceros críticos incompleto o informal	Q20	Zscaler	Refutada
H9	D4	Evaluación de terceros ausente o ad hoc en entidades importantes	Q21	Foro Económico Mundial	Sostenida parcialmente
H10	General	Sesgo de autocomplacencia entre madurez percibida y validada	Q24 frente a modelo	Proofpoint	Confirmada frente a la regla del mínimo (no frente a la media de dimensiones)
H11	D1	Asunción formal de la supervisión por delante de la capacidad de ejercerla	Q14 frente a Q13	EY Center for Board Matters (2025), divulgación sobre supervisión de IA en 80 empresas de la *Fortune 100*	Sin datos concluyentes (indicio compatible)
H12	D4	La concentración de proveedores agrava el riesgo agregado sin monitorización formal	Q20 y Q21	Consejo de Estabilidad Financiera (2026), informe sometido a consulta; Reglamento (UE) 2022/2554 (DORA), arts. 28 y 29	No contrastable

Certificarse ayuda, pero no basta.
La pregunta ya no es solo si una organización tiene buenos controles, sino si su Consejo sabe gobernar el riesgo que esos controles protegen.

Por eso el cumplimiento de NIS2 en España no se juega solo en el centro de operaciones de seguridad.
Se juega en la sala del Consejo.

Estudio de Madurez NIS2 ·
Center for the Governance of Change (CGC),
IE University, e ISMS Forum España, 2026.

© 2026, CGC Madrid, Spain
Fotografías: Unsplash, Shutterstock, Freepik.
Diseño: studioazola.com

Esta obra está sujeta a una licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional (CC BY-NC-SA 4.0). Para ver una copia de la licencia, visite creativecommons.org/licenses/by-nc-sa/4.0/deed.es

ie UNIVERSITY
CENTER FOR THE GOVERNANCE OF CHANGE

isms forum