MODELO DE MADUREZ DE RESILIENCIA ESTRUCTURAL NIS2

isms forum

ie UNIVERSITY
CENTER FOR THE GOVERNANCE OF CHANGE

MODELO DE MADUREZ DE RESILIENCIA ESTRUCTURAL NIS2

Documento Resumen — Versión 2.0

Una visión rápida del modelo, sus dimensiones y su escala de madurez

Versión 2.0 · Abril 2026 · Center for the Governance of Change at IE University · ISMS Forum Spain

Investigador Principal: Casimiro Juanes Calvo

1. Por qué este modelo

El problema que resuelve

La Directiva NIS2 cambia las reglas del juego. Por primera vez con este alcance, una directiva europea hace responsable directo al órgano de dirección (Art. 20), exige medidas de gestión de riesgos proporcionadas (Art. 21) y obliga a notificar incidentes en plazos cerrados (Art. 23). En España, la Ley de Coordinación y Gobernanza de la Ciberseguridad transpone NIS2 y requerirá que unas 20.000 entidades queden bajo la supervisión de las distintas autoridades competentes.

Las organizaciones disponen de marcos excelentes para evaluar *controles técnicos* — como NIST CSF, ISO 27001, CMMC y ENS. Lo que ningún marco existente responde es la pregunta que un CISO necesita poder contestar ante su Consejo: ***¿Cuál es nuestra madurez en el gobierno de la ciberseguridad?***

Ese vacío entre el cumplimiento técnico y la madurez organizativa es el que cubre este modelo.

Qué es y qué no es

Es una herramienta de diagnóstico organizativo que evalúa la madurez de gobierno de ciberseguridad. Permite identificar dónde está la organización, dónde debería estar según NIS2, y qué camino recorrer. No es una checklist legal. No es una auditoría técnica. No sustituye el cumplimiento normativo; lo complementa con una visión de gobernanza.

> *Este modelo no exime ni sustituye las obligaciones derivadas de NIS2, su transposición española o cualquier otra norma sectorial aplicable. Su uso es complementario al cumplimiento normativo.*

Cómo se diseñó

El modelo es resultado de varios meses de investigación aplicada (diciembre 2025 – abril 2026):

- Revisión sistemática de 74 documentos regulatorios y académicos.
- Co-diseño con expertos del sector y validación a través de dos talleres con 13 expertos.
- Validación cuantitativa por *Content Validity Index* — S-CVI/Ave global **0.917** (umbral de excelencia ≥ 0.90).
- Encuesta nacional a CISOs lanzada en abril de 2026 — datos preliminares se incorporarán al informe estratégico de junio.

2. Cómo está construido

Principios de diseño

El modelo se sustenta en siete principios que conviene conocer antes de leer las dimensiones:

- **Enfoque organizacional, no técnico.** Evalúa estructuras, procesos y gobernanza, no la implementación de controles concretos.
- **Alineamiento con NIS2.** Cada dimensión se mapea con artículos específicos de la Directiva (Arts. 20, 21 y 23).
- **Progresión lógica.** Cada nivel representa un salto en madurez, no solo un incremento cuantitativo.
- **Proporcionalidad.** Basado en principios, no en reglas. Los descriptores se interpretan según tamaño, sector y complejidad de cada organización (Art. 21.1 NIS2).
- ***Apply and explain.*** Filosofía heredada del King IV Code de Sudáfrica (2016): lo que importa es la *capacidad demostrada con evidencia*, no la coincidencia literal con un descriptor.
- **Aplicabilidad práctica.** Descriptores basados en comportamientos observables y evidencias verificables.
- **Alcance europeo, aplicación local.** Fundamentado en la Directiva (UE) 2022/2555 como texto primario; la arquitectura es replicable en cualquier estado miembro.

La gestión de incidentes atraviesa el modelo

La gestión de incidentes no vive en una sola dimensión. Se aborda desde la perspectiva que corresponde a cada una:

- **D1 — Gobernanza del incidente:** quién activa el protocolo de crisis, quién notifica al regulador (Art. 23), quién informa al Consejo y con qué plazos.
- **D2 — Riesgo materializado:** el incidente como input al ERM; lecciones que actualizan el apetito de riesgo.
- **D3 — Ejecución de la respuesta:** capacidad operacional real de contener, recuperar y documentar dentro de los plazos del Art. 23 (aviso 24h, notificación 72h, informe final 1 mes).

- D4 — **Incidentes en la cadena de suministro:** notificaciones de proveedores, obligaciones contractuales, riesgo de terceros materializado.
- D5 — **Capacidad humana y organizacional de gestión de incidentes y aprendizaje:** equipos entrenados, incorporación sistemática de lecciones aprendidas.

Estructura general

5 dimensiones × 4 subdimensiones × 5 niveles de madurez = un mapa que combina *profundidad* (qué evaluar) con *gradualidad* (cómo mejorar).

El nivel global de una organización es **el más bajo de sus subdimensiones**. El nivel no se evalúa con promedios, y la Alta Dirección debe ser consciente y supervisar los riesgos que puedan tener impacto material, que suelen ser su eslabón más débil.

3. Las 5 dimensiones

Cada dimensión cubre uno o varios dominios que NIS2 exige explícitamente. Cada una de las cinco dimensiones tiene cuatro subdimensiones cada una. Cada subdimensión describe lo que pretende verificarse.

D1 — Gobierno y Liderazgo de Ciberseguridad

Artículos NIS2: 20.1, 20.2, 21.2(a,f,h,j), 23

Evalúa el posicionamiento real del CISO, el *accountability* del Consejo, la integración estratégica de la ciberseguridad y la calidad del reporting. Es la dimensión donde NIS2 introduce su mayor cambio: la responsabilidad del Consejo es directa y personal.

- **D1.1 — Estructura y gobernanza de Ciberseguridad.** Verificar si existen los órganos, roles y capacidades de supervisión para que la ciberseguridad sea gestionada con autoridad real e influencia, no solo nominal.
- **D1.2 — Supervisión y accountability del Consejo.** Comprobar que el Consejo no solo recibe informes, sino que decide, exige evidencias y deja trazabilidad documental de su supervisión.
- **D1.3 — Integración estratégica y recursos.** Evaluar si la ciberseguridad participa en las decisiones estratégicas y de inversión, con presupuesto justificado en términos de riesgo.
- **D1.4 — Reporting y supervisión de capacidades.** Determinar si el reporte al Consejo es relevante para decidir y si se supervisan las capacidades que NIS2 exige.

D2 — Gestión de Riesgo Empresarial (ERM)

Artículos NIS2: 21.2(a), 20.1, 21.2(f)

Evalúa cómo el riesgo cibernético se integra en la gestión de riesgos corporativa, su metodología de análisis y cuantificación, y la capacidad de comunicarlo en lenguaje comparable al de los demás riesgos empresariales.

- D2.1 — **Integración con ERM corporativo.** Verificar que el riesgo ciber está en el mapa corporativo de riesgos, con la misma estructura y peso que los demás, no como silo técnico aislado.
- D2.2 — **Metodología de análisis de riesgos.** Comprobar que existe una metodología documentada y aplicada, con inventario de activos que incluye TI, OT, datos sensibles y dependencias críticas.
- D2.3 — **Cuantificación y comunicación de riesgos.** Evaluar si el riesgo ciber se expresa en términos financieros y de negocio comparables, suficientes para que el Consejo pueda decidir sobre inversiones y transferencia.
- D2.4 — **Evaluación de eficacia y auditoría.** Determinar si las medidas de mitigación se evalúan periódicamente mediante capacidad de auditoría independiente y se ajustan en función de los resultados.

D3 — Resiliencia Operacional y Continuidad

Artículos NIS2: 21.2(b,c), 23

Evalúa la capacidad de mantener operaciones críticas durante y después de un incidente, así como la coordinación con autoridades y grupos de interés externos en los plazos del Art. 23.

- D3.1 — **Inventario de servicios críticos y planes BCP/DRP.** Verificar que existe un inventario de servicios y activos críticos, BIA actualizado y planes de continuidad y recuperación con RTO/RPO definidos ex-ante.
- D3.2 — **Detección y respuesta a incidentes.** Evaluar la capacidad técnica y operacional de detectar, contener y recuperar — herramientas, cobertura y tiempos MTTD/MTTR.
- D3.3 — **Gestión de crisis y eficacia de recuperación.** Comprobar que los planes funcionan cuando se activan: simulacros, pruebas reales, equipo de crisis estratégico entrenado.
- D3.4 — **Coordinación externa.** Determinar si la organización cumple sus obligaciones de notificación regulatoria (Art. 23: 24h/72h/1 mes) y comunica eficazmente con clientes, terceros y autoridades.

D4 — Gestión de Terceros y Cadena de Suministro

Artículos NIS2: 21.2(d,e), 20.1

Evalúa la madurez en la gestión del riesgo de terceros — desde la identificación de proveedores críticos hasta la supervisión continua y la gestión de riesgos agregados de cadena.

- D4.1 — **Identificación y clasificación de terceros críticos.** Verificar que existe un inventario completo de terceros con criterios de criticidad documentados, no solo contractual sino por dependencia operacional.
- D4.2 — **Evaluación de ciberseguridad de terceros.** Evaluar si la ciberseguridad de proveedores críticos se valida con evidencia (certificaciones, auditorías, monitorización continua) y no solo declarativa.

- D4.3 — **Supervisión contractual y ciclo de vida.** Comprobar que existen cláusulas contractuales sólidas, supervisión durante la relación y procedimientos seguros de offboarding.
- D4.4 — **Gestión de riesgos agregados y concentración.** Determinar si la organización entiende y gestiona la concentración de riesgo en proveedores Tier 1 y los efectos cascada en su cadena.

D5 — Cultura y Capacidades Organizacionales

Artículos NIS2: 20.2, 21.2(e,f,g,i)

Evalúa los activos humanos y culturales que sostienen el resto del sistema: concienciación, talento, capacidad humana de respuesta y cultura de aprendizaje organizacional.

- D5.1 — **Concienciación y formación general.** Verificar que existe un programa de concienciación con phishing simulado, medición de efectividad y formación especializada por rol.
- D5.2 — **Talento y estrategia de capacidades ciber.** Evaluar si la organización tiene una estrategia consciente de talento — build/buy/partner — con gobernanza de la externalización y verificación de antecedentes para perfiles sensibles.
- D5.3 — **Capacidad de gestión de incidentes.** Comprobar que existe un equipo operativo entrenado para ejecutar la respuesta — distinto del equipo de crisis estratégico de D3.3 — con roles claros y simulacros regulares.
- D5.4 — **Cultura de responsabilidad y aprendizaje organizacional.** Determinar si la organización aprende sistemáticamente — de incidentes propios y de señales externas — y si los equipos no-técnicos aplican criterios de seguridad en sus decisiones por convicción, no por imposición.

4. Los 5 niveles de madurez

Cada nivel cambia la naturaleza de cómo se hacen las cosas, no solo cuántas se hacen.

N1 — Inicial / Reactivo Incumplimiento grave

Prácticas ad-hoc, dependientes de individuos. La organización reacciona a los incidentes sin anticipación.

N2 — En Desarrollo Insuficiente

Procesos documentados pero con aplicación inconsistente. Se reconoce la ciberseguridad como riesgo empresarial, pero la gobernanza es informal.

N3 — Establecido Umbral NIS2 · Propuesta para Entidades Importantes

Procesos estandarizados, supervisión activa, reporting regular al Consejo. **Es el nivel mínimo esperable** para cualquier organización dentro del perímetro NIS2.

N4 — Estratégico Excelencia esperada · Propuesta para Entidades Esenciales

Integración completa de la ciberseguridad en el gobierno corporativo. CISO en comités directivos, cuantificación de riesgos con metodología documentada, capacidad de anticipación parcial.

N5 — Optimizado Excelencia

Ciber-resiliencia como ventaja competitiva. La organización **anticipa disrupciones**, mantiene un portfolio de opciones estratégicas y demuestra legitimidad ante múltiples stakeholders.

Visualización del modelo como una oportunidad estratégica:

Cumplir es el mínimo. La pregunta es qué hay por encima.

N3 marca la línea de cumplimiento. N4 y N5 marcan el espacio en el que la ciberseguridad deja de ser una carga regulatoria y se convierte en una **capacidad estratégica**.

5. Siguientes pasos

Este documento es un resumen — el modelo completo, los descriptores detallados de cada nivel y la guía de autoevaluación están disponibles para las organizaciones que participen en la encuesta nacional. ***Si eres CISO o tienes responsabilidad de ciberseguridad en una organización española, tu contribución a la encuesta alimenta directamente el primer benchmark sectorial de preparación NIS2 en España.***

Encuesta nacional

Operativa hasta el ~20 de mayo de 2026. Resultados agregados se publicarán en el informe estratégico nacional en junio-julio de 2026.

Enlace ISMS Forum: https://es.surveymonkey.com/r/NIS2rrss

Documento elaborado por el equipo de investigación · Versión 2.0 · Abril 2026 · ISMS Forum Spain · Center for the Governance of Change, IE Universidad