



02/2026

08/10/2026

Juan Carlos Fernández Cela y José
Fuentes García

**Inteligencia económica y financiera en
la nueva Estrategia de Seguridad
Nacional 2026**

[Visitar la WEB](#)

[Recibir BOLETÍN ELECTRÓNICO](#)

Inteligencia económica y financiera en la nueva Estrategia de Seguridad Nacional 2026: de la conciencia del riesgo a una capacidad permanente del Estado

Resumen:

La revisión de la Estrategia de Seguridad Nacional ofrece a España la oportunidad de corregir una discontinuidad. Los riesgos económicos y financieros están reconocidos desde hace años, pero su tratamiento todavía no se ha consolidado como una capacidad transversal, estable y evaluable del Sistema de Seguridad Nacional. Este artículo propone incorporar expresamente la inteligencia económica (IE) y la inteligencia financiera (FININT), con funciones diferenciadas y convergencia analítica. La IE identifica dependencias, posiciones de control y vulnerabilidades en cadenas de suministro, tecnología, inversión, deuda, infraestructuras y contratos. También apoya la protección y la proyección de los intereses económicos estratégicos. La FININT reconstruye titularidades, activos, intermediarios, pagos, garantías y circuitos de financiación relevantes para la seguridad. Su integración permitiría construir una imagen nacional de exposición estratégica y mejorar la anticipación. El texto recupera el antecedente español del Sistema de Inteligencia Económica y propone desarrollarlo de manera descentralizada y gradual, con dirección política, productos comunes, geometría variable, comunicaciones seguras, cooperación público-privada y garantías jurídicas. La finalidad es reforzar la libertad de decisión del Estado sin convertir toda la actividad económica en objeto de seguridad.

Palabras clave:

Estrategia de Seguridad Nacional; inteligencia económica; inteligencia financiera; FININT; seguridad económica; coerción económica; dependencias estratégicas; infraestructuras críticas.

***NOTA:** Las ideas contenidas en los **Documentos Marco** son responsabilidad de sus autores, sin que reflejen necesariamente el pensamiento del IEEE o del Ministerio de Defensa.

Economic and financial intelligence in Spain's 2026 National Security Strategy: from risk awareness to a permanent state capability

Abstract:

The review of Spain's National Security Strategy offers Spain the opportunity to correct a discontinuity. Economic and financial risks have been recognised for years, yet they have still not been consolidated into a cross-cutting, stable and assessable capability within the National Security System. This article proposes the explicit incorporation of economic intelligence (EI) and financial intelligence (FININT) as distinct but analytically convergent functions. EI identifies dependencies, positions of control and vulnerabilities affecting supply chains, technology, investment, debt, infrastructure and contracts. It also supports the protection and projection of strategic economic interests. FININT reconstructs ownership, assets, intermediaries, payments, guarantees and financing circuits relevant to national security. Their integration would make it possible to develop a national picture of strategic exposure and strengthen anticipatory capacity. The article revisits Spain's earlier Economic Intelligence System and proposes its gradual development through a decentralised model combining political direction, common intelligence products, variable-geometry cooperation, secure communications, public-private collaboration and legal safeguards. The purpose is to strengthen the State's decision-making autonomy without turning all economic activity into a matter of national security.

Keywords:

National Security Strategy; economic intelligence; financial intelligence; FININT; economic security; economic coercion; strategic dependencies; critical infrastructure.

Cómo citar este documento:

FERNÁNDEZ CELA, Juan Carlos y FUENTES GARCÍA, José. *Inteligencia económica y financiera en la nueva Estrategia de Seguridad Nacional 2026: de la conciencia del riesgo a una capacidad permanente del Estado*. Documento Marco IEEE 02, 2026.

Introducción. Una carencia de arquitectura

La próxima Estrategia de Seguridad Nacional (ESN) se elabora en un entorno en el que seguridad, economía y tecnología forman un mismo espacio de competencia. El procedimiento aprobado por el Consejo de Seguridad Nacional el 24 de abril de 2025 exige analizar el entorno estratégico, concretar riesgos y amenazas, definir líneas de acción y optimizar los recursos existentes. También prevé la participación de todos los departamentos ministeriales, del Centro Nacional de Inteligencia, de las comunidades autónomas y de expertos procedentes del sector público, privado y científico¹.

El acuerdo no se limita a ordenar el procedimiento. Su exposición enfatiza el refuerzo de la disuasión y la defensa, el desarrollo de capacidades industriales, la gestión integral de crisis, la alerta temprana y la integración segura de información. También identifica la economía y la tecnología como vectores de influencia geopolítica. Este marco ofrece un cauce concreto para incorporar la inteligencia económica y la inteligencia financiera como capacidades diferenciadas y convergentes, no como una adición terminológica al catálogo de riesgos².

España dispone además de un antecedente claro. La Estrategia Española de Seguridad de 2011 propuso desarrollar un Sistema de Inteligencia Económica (SIE), en colaboración con el sector privado, para obtener y analizar información económica, financiera y empresarial relevante para la seguridad. La ESN de 2013 mantuvo esa orientación. Las estrategias de 2017 y 2021 ampliaron el tratamiento de la seguridad económica, las inversiones, las cadenas críticas y la tecnología, aunque la fórmula del SIE perdió continuidad y no se consolidó una función transversal reconocible³. El problema actual surge de esa distancia entre la identificación del riesgo y la organización de una capacidad permanente.

1 Orden PJC/521/2025, de 23 de mayo, por la que se publica el Acuerdo del Consejo de Seguridad Nacional de 24 de abril de 2025, por el que se aprueba el procedimiento para la elaboración de la nueva Estrategia de Seguridad Nacional. BOE núm. 126, 26 de mayo de 2025. <https://www.boe.es/eli/es/o/2025/05/23/pjc521>

2 Orden PJC/521/2025, de 23 de mayo, por la que se publica el Acuerdo del Consejo de Seguridad Nacional de 24 de abril de 2025, por el que se aprueba el procedimiento para la elaboración de la nueva Estrategia de Seguridad Nacional. BOE núm. 126, 26 de mayo de 2025. <https://www.boe.es/eli/es/o/2025/05/23/pjc521>

3 Gobierno de España, Estrategia Española de Seguridad. Una responsabilidad de todos (2011); Estrategia de Seguridad Nacional 2013; Estrategia de Seguridad Nacional 2017; Estrategia de Seguridad Nacional 2021. <https://www.lamoncloa.gob.es/serviciosdeprensa/paginas/postit/EstrategiaEspanolaDeSeguridad.aspx>; <https://www.dsn.gob.es/es/actualidad/sala-de-prensa/estrategia-seguridad-nacional-2021>. Instituto Español de Estudios Estratégicos (2016), El sistema de inteligencia económica en España, Documento de Trabajo DIEET07-2016. <https://www.defensa.gob.es/ceseden/-/el-sistema-de-inteligencia-economica-en-espa%C3%B1a>

La trayectoria es relevante por una razón adicional. La mención de 2011 no planteaba una agencia aislada, sino un sistema construido con el sector privado y orientado a mejorar la decisión del Estado. Ese planteamiento anticipaba dos rasgos que hoy resultan centrales: el conocimiento decisivo se encuentra distribuido y la seguridad económica exige continuidad más allá de una crisis concreta. La propuesta perdió visibilidad institucional, pero el entorno ha evolucionado en la dirección que la hacía necesaria.

Las sanciones, la competencia por tecnologías críticas, el control de inversiones y la vulnerabilidad de las cadenas de suministro han ampliado el número de decisiones públicas que requieren una lectura integrada. El Informe Anual de Seguridad Nacional 2025 confirma la creciente relevancia de este espacio de riesgos económicos, tecnológicos y de suministro⁴.

La discontinuidad no equivale a ausencia de capacidades. España cuenta con organismos de inteligencia, supervisores, autoridades sectoriales, fuerzas y cuerpos de seguridad, órganos de control de inversiones y exportaciones, registros administrativos y operadores privados que producen información de alto valor. El Sepblac ejerce como Unidad de Inteligencia Financiera española dentro del marco jurídico específico de prevención del blanqueo de capitales y de la financiación del terrorismo⁵. Otros órganos analizan competencia, mercados, inversiones, solvencia, infraestructuras, comercio exterior, amenazas híbridas o protección de tecnologías.

La debilidad se encuentra en la falta de un producto común, al menos en un nivel no clasificado, que relacione esas representaciones parciales cuando una exposición económica puede afectar a la seguridad nacional.

Este mapa institucional puede modificarse si culmina la reforma aprobada en primera vuelta por el Consejo de Ministros el 28 de julio de 2026. El anteproyecto prevé crear la Autoridad Nacional de Integridad Financiera (ANIFI) como autoridad administrativa independiente, construirla sobre la estructura del actual FROB e integrar en ella funciones de Unidad de Inteligencia Financiera, supervisión e inspección, potestad

4 Departamento de Seguridad Nacional, Informe Anual de Seguridad Nacional 2025 (2026).

<https://www.dsn.gob.es/es/actualidad/sala-de-prensa/IASN2025>

5 Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo; Ley Orgánica 9/2022, de 28 de julio; Sepblac, Unidad de Inteligencia Financiera y estructura organizativa.

<https://www.sepblac.es/es/sobre-el-sepblac/organizacion/estructura-organizativa/>

sancionadora, sanciones financieras internacionales y prevención de la financiación de la proliferación. También sería el interlocutor español ante AMLA⁶.

La propuesta refuerza la especialización institucional, pero no equivale al SIE defendido en este artículo. Su ámbito anunciado es sectorial y jurídicamente tasado, mientras que la ESN necesita relacionar exposiciones financieras con dependencias industriales, tecnológicas, inversoras, contractuales y territoriales. Si finalmente se constituye, ANIFI podría actuar como nodo especializado del sistema, sin absorber la coordinación estratégica ni borrar la separación entre inteligencia financiera, supervisión, inspección e investigación penal.

Seguridad económica, inteligencia económica e inteligencia financiera ocupan niveles diferentes. La seguridad económica define el objetivo político de preservar funciones, capacidades y margen de decisión. La IE y la FININT producen conocimiento para orientar ese objetivo. La política industrial, el control de inversiones, la supervisión financiera, la política comercial y la persecución penal aplican instrumentos jurídicos propios. Mantener esta distinción evita atribuir a la inteligencia funciones de regulación o intervención y permite concentrar su aportación en la anticipación, la contextualización y la evaluación de alternativas.

A efectos de este artículo, la inteligencia económica se entiende como una función sistemática de obtención, análisis, protección y difusión de información relevante para decisiones económicas estratégicas. Comprende la protección de activos y capacidades críticas, la detección de oportunidades y amenazas, y el apoyo a la proyección de los intereses nacionales. Su eficacia depende de la interacción coordinada entre Administración, empresa, universidad y centros tecnológicos.

La FININT se emplea aquí en sentido funcional para designar el análisis de flujos, activos, titularidades, intermediarios, pagos, garantías y mecanismos financieros relevantes para la seguridad. Esta acepción no convierte la FININT en sinónimo de la actividad de una UIF ni altera las competencias legales de los organismos que producen la información dentro del Sistema de Seguridad Nacional⁷. En este contexto, tampoco debe reducirse al blanqueo y la financiación del terrorismo. Sirve para atribuir control y seguir la

6 Gobierno de España, Consejo de Ministros (2026), «Reforma integral del marco de prevención del blanqueo de capitales y la financiación del terrorismo», referencia de 28 de julio de 2026.
<https://www.lamoncloa.gob.es/consejodeministros/referencias/paginas/2026/20260728-referencia-rueda-de-prensa-ministros.aspx>

7 Ley 36/2015, de 28 de septiembre, de Seguridad Nacional. <https://www.boe.es/eli/es/l/2015/09/28/36>

activación de posiciones financieras relevantes para sanciones, proliferación, interferencia o evasión.

Las dos funciones observan dimensiones distintas de una misma estructura. La IE permite localizar dependencias, posiciones de control, conocimiento crítico y puntos de sustitución. La FININT ayuda a establecer quién financia, garantiza, intermedia, cobra o se beneficia, y cómo se conectan actores estatales, empresariales y criminales. Su convergencia puede responder preguntas que suelen quedar fragmentadas: qué función nacional está en juego, de qué activo o proveedor depende, dónde se concentra el control, qué opacidad impide conocerlo, qué actor puede explotar la vulnerabilidad, mediante qué canal y con qué efecto sobre la libertad de acción de España.

Sería, por tanto, adecuado que la nueva ESN pudiera reconocer la IE y la FININT como capacidades transversales, definir los productos que han de aportar al ciclo de decisión y ordenar un desarrollo institucional posterior. Ese desarrollo puede recuperar el concepto de SIE, siempre que se configure como un sistema federado y gradual, no como la absorción de competencias ya atribuidas. La estrategia debe fijar dirección política, objetivos y plazos; el instrumento posterior tendrá que concretar autoridades, composición, reglas de acceso, comunicaciones, recursos y garantías.

La cuestión decisiva es de mando y control. Un sistema necesita prioridades aprobadas, requerimientos de información, responsables de producción, procedimientos de integración, un destinatario político y un circuito de retorno que permita saber si el análisis modificó una decisión. Sin esa cadena, la coordinación se reduce al intercambio ocasional de datos. Con ella, los organismos pueden conservar su autonomía y producir una imagen común sin trasladar expedientes, duplicar bases de datos o alterar custodias legales.

El límite es igualmente importante. La inflación, la productividad, la competencia o la inversión extranjera pueden plantear problemas graves sin alcanzar por ello la condición de riesgo para la seguridad nacional. La intervención se justifica cuando concurren concentración, dificultad de sustitución, opacidad, capacidad de explotación y una magnitud de efecto suficiente para comprometer funciones esenciales, autonomía tecnológica, sostenimiento, defensa, energía, telecomunicaciones, acción exterior o resiliencia social. Una ESN rigurosa debe ampliar su capacidad de observación y mantener una delimitación precisa de su objeto.

Por qué la interdependencia exige una capacidad integrada

De la eficiencia al uso estratégico de la interdependencia

Durante varias décadas, la interdependencia fue analizada sobre todo como una fuente de eficiencia, especialización y reducción de costes. Las sanciones vinculadas a la guerra de Ucrania, la disputa tecnológica entre Estados Unidos y China, las restricciones a la exportación, la presión sobre energía y materias primas y la regionalización de cadenas han mostrado su dimensión estratégica. Las redes económicas distribuyen beneficios, pero también capacidad de observación, exclusión y condicionamiento. Farrell y Newman denominaron efecto panóptico a la posibilidad de extraer información desde nodos centrales y efecto de estrangulamiento a la capacidad de negar el acceso a esos nodos⁸.

España participa intensamente en redes europeas y globales sin controlar de forma directa la mayoría de sus nodos centrales. La respuesta realista consiste en conocer la posición propia, las concentraciones críticas y los costes de sustitución. La IE identifica dependencias y opciones; la FININT revela financiación, beneficiarios y canales de presión. Esta lectura evita tanto la promesa de una autonomía absoluta como la aceptación pasiva de exposiciones que sí pueden reducirse.

La posición de España tampoco puede medirse únicamente por el volumen de importaciones o exportaciones. Dos relaciones comerciales de tamaño similar pueden producir vulnerabilidades muy distintas si una depende de un proveedor único, de una licencia revocable, de una moneda de financiación externa o de un servicio digital sin sustituto inmediato. La inteligencia debe identificar esos puntos de asimetría y estimar cuánto tiempo necesita el país para sustituirlos. El dato central es la capacidad de reacción, no la mera existencia de interdependencia.

La coerción puede operar sin una sanción formal

La coerción económica comprende sanciones, controles de exportación y restricciones de inversión, pero también puede adoptar formas menos visibles. Retrasos regulatorios, retirada de financiación, presión sobre proveedores, licencias de tecnología, precios discriminatorios, litigios, ejecución de garantías o movimientos coordinados sobre la confianza de un activo pueden alterar decisiones sin una directriz pública fácilmente

⁸ Farrell, H. y Newman, A. L. (2019), «Weaponized Interdependence: How Global Economic Networks Shape State Coercion», *International Security*, 44(1), pp. 42–79. https://doi.org/10.1162/isec_a_00351

atribuible. La acción suele distribuirse entre administraciones, bancos, fondos, aseguradoras, empresas estatales, operadores logísticos y sociedades interpuestas.

El análisis estratégico debe reconstruir la arquitectura que hace posible la presión. La nacionalidad formal de una empresa o la localización física de una infraestructura aportan información insuficiente cuando la propiedad, el control operativo, la financiación y la jurisdicción contractual se encuentran en países diferentes. La geografía del poder económico se expresa en derechos, dependencias y posiciones de intermediación, además de en activos materiales.

La alerta temprana exige observar señales que por separado pueden parecer ordinarias. Cambios simultáneos de condiciones crediticias, concentración de compras sobre un componente, litigios coordinados, incremento de primas de seguro, operaciones societarias opacas o presión regulatoria sobre una ruta logística pueden formar un patrón. La IE aporta el contexto sectorial y geopolítico; la FININT ayuda a comprobar vínculos, secuencias y beneficiarios. La integración reduce el tiempo necesario para distinguir una perturbación de mercado de una acción deliberada.

Tecnología, conocimiento y datos como activos de seguridad

La competencia tecnológica ha desplazado el foco desde el producto final hacia el ecosistema que lo hace posible. Capital, personal especializado, propiedad intelectual, fabricación, software, datos, servicios en la nube, minerales, maquinaria y estándares forman cadenas cuya interrupción puede neutralizar una capacidad completa. La Estrategia Europea de Seguridad Económica de 2023 organiza la evaluación alrededor de cadenas de suministro, infraestructuras, seguridad tecnológica y coerción económica, con criterios de proporcionalidad y precisión⁹. La evaluación inicial de tecnologías críticas priorizó semiconductores avanzados, inteligencia artificial, tecnologías cuánticas y biotecnología¹⁰.

La IE debe distinguir qué capacidades carecen de sustituto, qué empresas concentran conocimiento, qué contratos permiten transferirlo y qué dependencias convierten una perturbación comercial en pérdida de autonomía. En defensa, esta lectura conecta la base industrial y tecnológica con el sostenimiento. Munición, repuestos, consumibles,

⁹ Comisión Europea y Alto Representante (2023), Joint Communication on a European Economic Security Strategy, JOIN(2023) 20 final, 20 de junio de 2023.

¹⁰ Comisión Europea (2023), Recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States, C(2023) 6689 final, 3 de octubre de 2023.

software, licencias, datos técnicos, mantenimiento y proveedores de segundo o tercer nivel pueden constituir puntos de bloqueo más relevantes que la plataforma principal. El análisis debe traducir la exposición en consecuencias operativas: qué capacidad deja de estar disponible, durante cuánto tiempo y con qué alternativas.

La seguridad de la investigación forma parte de este mismo problema. Las transferencias de conocimiento pueden producirse mediante adquisiciones, inversión en empresas emergentes, contratación de personal, acceso remoto a datos, proyectos conjuntos o dependencia de equipamiento y plataformas. Una política eficaz debe diferenciar la colaboración legítima de los vínculos que crean exposición sobre tecnologías sensibles. La respuesta requiere orientación comprensible para investigadores y empresas, evaluación proporcionada y canales de consulta, además de controles formales.

Las infraestructuras críticas también son estructuras financieras y contractuales

Puertos, redes energéticas, centros de datos, cables submarinos, satélites, sistemas de pago y nodos logísticos no se controlan únicamente mediante la propiedad directa. Concesiones, deuda garantizada, derechos de veto, contratos de operación, pactos de accionistas, seguros, garantías y cláusulas de jurisdicción distribuyen capacidades de decisión entre actores situados en distintos países. La geografía material de la infraestructura y la geografía jurídica y financiera de su control rara vez coinciden por completo.

La IE identifica la función crítica, los activos y las alternativas. La FININT aporta trazabilidad sobre financiación, garantías, pagos y beneficiarios efectivos. El objetivo consiste en reconocer aquellos contratos y estructuras en los que una concentración de derechos puede condicionar la continuidad de una función esencial. Esta dimensión permanece poco visible en las estrategias generales, aunque determina quién puede bloquear, sustituir, acelerar o encarecer una respuesta.

El análisis contractual debe atender a derechos de terminación, cambio de control, ejecución de garantías, *step-in rights*, licencias, mantenimiento, acceso a datos y resolución de disputas. Ninguna cláusula aislada demuestra una vulnerabilidad; el riesgo aparece cuando varias de ellas concentran capacidad de decisión en un actor externo y las alternativas requieren plazos incompatibles con la continuidad del servicio. La evaluación debe conectar el contrato con la operación real y con los escenarios de crisis.

Deuda, inversión y exposición en terceros países

La seguridad de España depende también de espacios exteriores. La financiación de infraestructuras, la deuda soberana, los créditos a empresas públicas y las garantías sobre activos estratégicos pueden alterar la capacidad de decisión de países relevantes para la energía, las comunicaciones, las rutas marítimas, las materias primas o la estabilidad regional. El riesgo aparece cuando la estructura financiera concentra derechos, reduce alternativas, facilita la apropiación de rentas o permite condicionar decisiones soberanas.

El análisis de deuda estratégica debe ir más allá de los agregados macroeconómicos y examinar acreedores, moneda, vencimientos, garantías, contratos asociados, jurisdicción, refinanciación y conexión con activos físicos. La misma lógica se aplica a la inversión extranjera. Una operación beneficiosa puede generar una dependencia difícil de revertir si afecta a tecnología dual, datos, mantenimiento o infraestructura insustituible. La inteligencia permite discriminar entre casos y evita convertir el origen extranjero del capital en una presunción de amenaza.

Para España, esta evaluación exterior tiene una dimensión preventiva y otra de política exterior. Permite anticipar cómo una crisis de deuda, una concesión problemática o una refinanciación pueden afectar a socios relevantes, pero también orientar la cooperación, la financiación alternativa y la diplomacia económica. La IE no se limita a proteger el mercado interno. También ayuda a proyectar intereses, identificar oportunidades y sostener relaciones económicas que reducen vulnerabilidades propias y de los socios.

Amenazas distintas que comparten infraestructuras financieras

Terrorismo, proliferación, crimen organizado, evasión de sanciones, corrupción, ciberataques y operaciones de influencia responden a lógicas distintas, pero con frecuencia utilizan las mismas sociedades, proveedores de servicios, plataformas de pago, redes de comercio y jurisdicciones. Criptoactivos, activos tokenizados¹¹ y finanzas descentralizadas añaden velocidad y fragmentación, aunque siguen conectados con entidades, monedas y servicios del sistema financiero tradicional.

La FININT permite reconstruir esas conexiones. En el nivel estratégico, su contribución puede materializarse mediante evaluaciones agregadas sobre tendencias, actores,

¹¹ Activos tokenizados: representaciones digitales de activos o de derechos sobre ellos mediante tokens, normalmente registrados y transferidos en infraestructuras de registro distribuido.

métodos de elusión y exposición sectorial, elaboradas y compartidas por los cauces legalmente previstos. La nueva arquitectura europea contra el blanqueo y la financiación del terrorismo, con AMLA y una coordinación reforzada de las UIF, incrementará la necesidad de interoperabilidad conforme a los estándares internacionales aplicables¹². Esa cooperación debe respetar la finalidad, la clasificación y las restricciones propias de cada fuente.

La separación funcional protege la legitimidad del sistema. La información obtenida para supervisión, inteligencia, investigación penal o cumplimiento normativo responde a bases jurídicas y finalidades distintas. La integración estratégica no autoriza una circulación indiscriminada. Puede apoyarse en productos agregados, indicadores, tipologías y alertas construidas por la autoridad competente. Esta solución permite elevar conocimiento al nivel político sin desnaturalizar la fuente ni trasladar datos personales innecesarios.

La empresa privada dentro del perímetro efectivo de seguridad

Buena parte de las capacidades críticas pertenece o está operada por empresas de telecomunicaciones, energía, banca, logística, nube, datos, defensa, seguros, auditoría, pagos y transporte. El Estado necesita su conocimiento, mientras conserva la responsabilidad de definir el interés nacional. La cooperación debe permitir que la Administración comparta amenazas, prioridades y tipologías, y que las empresas aporten señales tempranas sobre proveedores, adquisiciones, presiones, impagos, alteraciones regulatorias y oportunidades estratégicas.

Dos fallos reducen habitualmente el valor de esa relación. El primero es la cooperación ocasional, activada cuando la crisis ya es visible. El segundo es el foro ceremonial sin continuidad ni retorno. Un SIE útil exige niveles de acceso, comunicaciones seguras, periodicidad, responsables, productos y resultados verificables. Las pymes requieren una atención específica porque algunas concentran conocimientos o componentes esenciales, pero carecen de recursos para sostener por sí mismas capacidades avanzadas de protección e inteligencia.

12 Reglamento (UE) 2024/1620, por el que se crea la Autoridad de Lucha contra el Blanqueo de Capitales y la Financiación del Terrorismo; Reglamento (UE) 2024/1624; Directiva (UE) 2024/1640. Financial Action Task Force, The FATF Recommendations, Recomendación 29, versión actualizada. <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html>; Egmont Group of Financial Intelligence Units, Charter. <https://egmontgroup.org/egmont-resources/egmont-group-charter/>

La confianza no puede imponerse mediante una obligación genérica de compartir información. Las empresas necesitan conocer la finalidad del intercambio, el tratamiento de la información sensible y el beneficio que obtendrán. Alertas contextualizadas, guías sectoriales, puntos de contacto y sesiones reservadas pueden generar un circuito de reciprocidad. El Estado recibe señales tempranas y los operadores mejoran su capacidad de protección.

Modelos comparados y lecciones para España

La comparación internacional requiere cautela. Una estrategia de seguridad nacional, una política de seguridad económica y una estructura de inteligencia económica y financiera son instrumentos diferentes. La Unión Europea fija buena parte del marco jurídico que España debe aplicar; Francia combina dirección central y despliegue territorial; Alemania articula protección económica con capacidades existentes; Japón ha convertido prioridades de seguridad económica en instrumentos legislativos; Reino Unido y Estados Unidos integran con especial intensidad seguridad, empresa y finanzas; Canadá ofrece una experiencia útil en seguridad de la investigación. Ningún modelo puede trasladarse de forma automática.

La Unión Europea proporciona el marco común. Su Estrategia de Seguridad Económica organiza la acción en torno a la promoción de la competitividad, la protección frente a riesgos y la cooperación con socios. El control de inversiones, el Instrumento Anticoerción, la evaluación de tecnologías críticas, la resiliencia de entidades esenciales y el paquete AML/CFT forman un ecosistema en expansión¹³. Para España, la consecuencia es directa: una capacidad nacional debe producir evaluaciones compatibles con la arquitectura europea y, al mismo tiempo, identificar exposiciones propias que no siempre quedan visibles en una agregación comunitaria.

La arquitectura europea está formada por piezas con mandatos diferentes. Dentro del Servicio Europeo de Acción Exterior, el Centro de Inteligencia y de Situación de la Unión Europea (EU INTCEN) produce análisis para la decisión europea a partir de aportaciones de los Estados miembros, delegaciones, misiones, imágenes de satélite y fuentes

13 Comisión Europea y Alto Representante (2023), Joint Communication on a European Economic Security Strategy, JOIN(2023) 20 final, 20 de junio de 2023. Reglamento (UE) 2024/1620; Reglamento (UE) 2024/1624; Directiva (UE) 2024/1640. Reglamento (UE) 2023/2675, relativo a la protección de la Unión y de sus Estados miembros frente a la coerción económica ejercida por terceros países.

abiertas¹⁴. OLAF realiza investigaciones administrativas sobre fraude, corrupción y otras conductas que afectan a los intereses financieros de la Unión¹⁵. La EUIPO alberga el Observatorio Europeo de las Vulneraciones de los Derechos de Propiedad Intelectual, una red que genera conocimiento, difunde buenas prácticas y apoya la aplicación de los derechos de propiedad intelectual¹⁶. Su información es relevante para proteger tecnología, marcas y otros activos intangibles, pero el Observatorio no es una unidad de inteligencia financiera.

En Europol, el Centro Europeo contra el Crimen Financiero y Económico (EFECC) concentra capacidades de apoyo operativo y análisis sobre delincuencia económica y financiera. En su seno se ubica el secretariado del Europol Financial Intelligence Public Private Partnership (EFIPPP), que Europol define como el primer mecanismo transnacional de intercambio de información establecido en materia de lucha contra el blanqueo de capitales y la financiación del terrorismo¹⁷. Las UIF, por su parte, intercambian inteligencia financiera dentro de su marco legal, y AMLA asume funciones europeas de coordinación y supervisión.

Considerar estas entidades fuentes, productoras o socias especializadas es útil; presentarlas como una única comunidad europea de inteligencia económica o FININT ocultaría diferencias de mandato, finalidad y acceso que España debe respetar al diseñar su interoperabilidad.

Japón muestra cómo un documento marco puede traducirse en instrumentos. La Estrategia de Seguridad Nacional de 2022 y la Ley de Promoción de la Seguridad Económica establecen mecanismos sobre suministros críticos, infraestructuras esenciales, tecnologías sensibles y patentes¹⁸. La lección transferible no procede de

14 Servicio Europeo de Acción Exterior y Estado Mayor de la Unión Europea, «Single Intelligence Analysis Capacity: ensuring strategic situational awareness», Impetus, núm. 28.

https://www.eeas.europa.eu/sites/default/files/documents/eums_impetus_28_final_web.pdf

15 Oficina Europea de Lucha contra el Fraude (OLAF), «What we do». https://anti-fraud.ec.europa.eu/about-us/what-we-do_en

16 Reglamento (UE) núm. 386/2012, por el que se encomiendan a la EUIPO funciones relacionadas con el respeto de los derechos de propiedad intelectual; EUIPO, European Observatory on Infringements of Intellectual Property Rights. <https://www.euiipo.europa.eu/en/observatory>

17 Europol, European Financial and Economic Crime Centre (EFECC); Europol Financial Intelligence Public Private Partnership (EFIPPP). <https://www.europol.europa.eu/about-europol/european-financial-and-economic-crime-centre-efecc>; <https://www.europol.europa.eu/media-press/newsroom/news/financial-institutions-and-law-enforcement-enhance-their-cooperation>

18 Gobierno de Japón (2022), National Security Strategy of Japan, 16 de diciembre de 2022.

https://www.mod.go.jp/en/d_policy/basis/index.html; Act on the Promotion of Ensuring National Security through Integrated Implementation of Economic Measures, Ley núm. 43 de 2022.

<https://www.japaneselawtranslation.go.jp/en/laws/view/4716/en>

rasgos culturales difíciles de comparar, sino de la continuidad entre doctrina, legislación, autoridades y calendario.

Alemania ofrece un camino diferente. Su Estrategia de Seguridad Nacional de 2023 adoptó la seguridad integrada y la Estrategia Nacional de Protección Económica aprobada en marzo de 2026 desarrolla la protección de empresas, investigación, innovación y cadenas de valor frente a amenazas físicas, digitales e híbridas¹⁹. Este caso demuestra que pueden coordinarse capacidades existentes sin crear necesariamente una gran organización nueva, siempre que existan mandato, relación con las empresas y medidas de implementación.

Francia aporta una experiencia administrativa estable. El SISSE diseña y coordina la política de seguridad económica y cuenta con una red territorial de delegados bajo la autoridad de los prefectos de región²⁰. Su valor para España reside en combinar dirección central, detección próxima al activo y acompañamiento a empresas. La estructura territorial francesa no es trasladable, pero sí la idea de que adquisiciones, pérdida de proveedores o presiones sobre centros tecnológicos suelen detectarse antes en el entorno productivo que en la sede central de la Administración.

Reino Unido y Estados Unidos muestran la utilidad estratégica de la información financiera. La revisión integrada británica conecta resiliencia, coerción y relación con el sector privado, mientras la UK Financial Intelligence Unit analiza y difunde comunicaciones de actividad sospechosa dentro de su marco legal²¹.

En Estados Unidos, el Tesoro integra sanciones, inteligencia y protección de la integridad financiera; su Office of Intelligence and Analysis forma parte de la comunidad de inteligencia. La Estrategia de Seguridad Nacional de 2025 vuelve a situar la seguridad económica como fundamento de la seguridad nacional²². La escala institucional de

19 Gobierno Federal de Alemania (2023), National Security Strategy. <https://www.bundesregierung.de/breg-de/aktuelles/national-security-strategy-2196356>; Gobierno Federal de Alemania (2026), Nationale Wirtschaftsschutzstrategie, aprobada el 18 de marzo de 2026. <https://www.bundesregierung.de/breg-de/aktuelles/kabinett-wirtschaftsschutz-2412548>

20 Direction générale des Entreprises, Service de l'information stratégique et de la sécurité économiques (SISSE) y red territorial DISSE. <https://www.entreprises.gouv.fr/service-de-linformation-strategique-et-de-la-securite-economiques-sisse>

21 Gobierno del Reino Unido (2023), Integrated Review Refresh 2023. <https://www.gov.uk/government/publications/integrated-review-refresh-2023-responding-to-a-more-contested-and-volatile-world>; National Crime Agency, UK Financial Intelligence Unit. <https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/money-laundering-and-illicit-finance/ukfiu>

22 The White House (2025), National Security Strategy. <https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf>; U.S. Department of the Treasury, Office of Terrorism and Financial Intelligence. <https://home.treasury.gov/about/offices/terrorism-and-financial-intelligence>; Office of Intelligence and Analysis. <https://home.treasury.gov/about/offices/terrorism-and-financial-intelligence/oia>

ambos países no es trasladable, pero sí la conexión regular entre análisis financiero y decisión estratégica.

Canadá resulta especialmente útil para la protección del conocimiento. El Canadian Security Intelligence Service (CSIS) ha desarrollado orientación pública para empresas, investigadores e inversores, y participa en la aplicación de políticas de seguridad de la investigación. La política sobre investigación en tecnologías sensibles y vínculos preocupantes establece controles focalizados sobre financiación federal, y la iniciativa Secure Innovation difunde pautas de mitigación frente al espionaje económico²³. La enseñanza para España consiste en combinar protección, formación y diálogo con universidades y empresas sin cerrar la cooperación científica legítima.

Los casos también muestran dos caminos institucionales. Francia hace visible un centro coordinador y una red territorial. Alemania distribuye la responsabilidad entre estructuras existentes y refuerza la cultura de protección en empresas e investigación. Japón vincula estrategia y legislación; Canadá enfatiza la prevención y la orientación pública; Reino Unido y Estados Unidos conectan el dato financiero con la decisión de seguridad. España podría combinar elementos de esos caminos: dirección política reconocible, ejecución federada, capacidad territorial y una interfaz estable con el tejido productivo.

Tabla 1. Modelos comparados y lecciones útiles para España

Actor	Encaje	Mecanismo principal	Lección para España
Unión Europea	Estrategia de Seguridad Económica y marco AML/CFT	Evaluación de riesgos, tecnología crítica, inversión, anticoerción y AMLA	Alinear la capacidad nacional con el sistema europeo y conservar una lectura específica de la exposición española
Japón	Seguridad económica dentro de la NSS de 2022	Ley sobre suministros, infraestructuras, patentes y tecnología	Vincular doctrina, instrumentos, responsables y calendario
Alemania	Seguridad integrada y estrategia de protección económica de 2026	Protección de empresas, I+D y cadenas de valor	Coordinar capacidades existentes mediante un desarrollo técnico evaluable
Francia	Política administrativa estable de seguridad económica	SISSE central y red territorial DISSE	Combinar dirección política con detección próxima a empresas y activos
Reino Unido	Revisión integrada, resiliencia y lucha contra finanzas ilícitas	Interfaz público-privada y UKFIU	Separar funciones y asegurar productos comunes y canales estables

23 Canadian Security Intelligence Service, Public Report 2024. <https://www.canada.ca/en/security-intelligence-service/corporate/publications/csis-public-report-2024.html>; Gobierno de Canadá, Policy on Sensitive Technology Research and Affiliations of Concern. <https://ised-isde.canada.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/sensitive-technology-research-and-affiliations-concern/policy-sensitive-technology-research-and-affiliations-concern>; Five Eyes Secure Innovation initiative. <https://www.canada.ca/en/security-intelligence-service/news/2024/10/five-eyes-intelligence-partners-launch-shared-security-advice-initiative-for-tech-companies-researchers-and-investors.html>

Actor	Encaje	Mecanismo principal	Lección para España
Estados Unidos	Seguridad económica como dimensión de seguridad nacional	Tesoro, sanciones e inteligencia financiera estratégica	Conectar análisis financiero con política exterior y seguridad
Canadá	Protección de innovación e investigación	Orientación pública, política STRAC y Secure Innovation	Extender la formación y la protección a universidades, inversores y pymes tecnológicas

Fuente: elaboración propia a partir de las estrategias y fuentes oficiales.

El examen comparado permite identificar cinco rasgos recurrentes. Primero, un mandato político reconocible. Segundo, un nodo o procedimiento capaz de integrar información sin borrar responsabilidades. Tercero, una relación estable con empresas, universidades y centros tecnológicos. Cuarto, productos que convierten el análisis en decisiones sobre inversión, tecnología, sanciones, protección de activos o respuesta a crisis. Quinto, separación entre inteligencia estratégica, supervisión, investigación penal y apoyo empresarial. La principal conclusión es institucional: las capacidades se debilitan cuando la coordinación depende de relaciones personales y desaparece de la evaluación pública.

Propuestas para la Estrategia de Seguridad Nacional 2026

A la luz de lo expuesto, parece razonable pensar que la ESN debería fijar doctrina, prioridades, gobernanza y obligaciones de desarrollo. No necesita describir un organigrama completo, pero sí evitar una fórmula genérica que pudiera, una vez más, aplazar la implementación. Las siguientes siete líneas permiten convertir el reconocimiento de la IE y la FININT en una capacidad evaluable.

Reconocimiento expreso y desarrollo gradual de un SIE

La estrategia debería nombrar la inteligencia económica y la inteligencia financiera como capacidades transversales de apoyo a la anticipación, la prevención, la gestión de crisis y la decisión estratégica. También debería recuperar el concepto de Sistema de Inteligencia Económica, entendido como un marco federado para integrar productos y no como una nueva autoridad con acceso indiscriminado a la información. Esta formulación reconoce la trayectoria iniciada en 2011 y corrige la pérdida de continuidad posterior.

La ESN puede ordenar un plan de implementación con plazo definido. Una primera célula de planeamiento debería inventariar capacidades, precisar productos, identificar vacíos, proponer reglas de coordinación y comparar alternativas organizativas. El diseño definitivo se adoptaría después de escuchar a organismos competentes, grandes

operadores, pymes estratégicas, universidades y centros tecnológicos. Este desarrollo gradual reduce el riesgo de crear una estructura nominal sin doctrina ni recursos.

El sistema debería respetar seis principios: dirección política al nivel adecuado, con capacidad efectiva de mando y control; competencias distribuidas y responsabilidades claras; participación público-pública y público-privada; geometría variable según la necesidad de conocer; comunicaciones seguras; y metodología común con trazabilidad. La Junta Interministerial de Material de Defensa y Doble Uso (JIMDDU) ofrece una analogía limitada pero útil. Demuestra que un órgano interministerial puede evaluar operaciones desde perspectivas diferentes y elevar una posición coordinada²⁴. Su objeto, régimen jurídico y decisiones no son trasladables al SIE, pero su lógica colegiada merece ser estudiada.

El despliegue podría organizarse en tres etapas. La primera elaboraría el inventario de capacidades, el marco conceptual y dos o tres productos piloto sobre exposiciones prioritarias. La segunda probaría procedimientos de cooperación con operadores y universidades, incluida la dimensión territorial. La tercera evaluaría resultados y propondría el encaje estable. Cada etapa debería cerrar con una decisión explícita sobre continuidad, recursos y correcciones. Así se evita que el SIE vuelva a quedar reducido a una declaración programática.

Una evaluación nacional de exposición económico-financiera

El producto principal debería ser una evaluación periódica dirigida al nivel político que integre dependencias económicas, tecnológicas, financieras, contractuales y territoriales. Su unidad de análisis sería la cadena mediante la cual una vulnerabilidad puede convertirse en efecto estratégico. La secuencia puede expresarse de forma sencilla: función crítica, dependencia, concentración, opacidad, actor, canal de explotación, efecto y respuesta disponible.

La evaluación debe superponer dos mapas. El primero representa dependencias, derechos de control, tecnología y puntos de bloqueo. El segundo reconstruye financiación, intermediarios, garantías, pagos y beneficiarios. La superposición permite distinguir una dependencia gestionable de una vulnerabilidad explotable y una

²⁴ Real Decreto 679/2014, de 1 de agosto, por el que se aprueba el Reglamento de control del comercio exterior de material de defensa, de otro material y de productos y tecnologías de doble uso.

<https://www.boe.es/buscar/act.php?id=BOE-A-2014-8926>

infraestructura localizada en España de una capacidad controlada desde otra jurisdicción.

Los indicadores deberían medir concentración, sustituibilidad, tiempo de reposición, exposición jurisdiccional, control societario, vencimientos, garantías y centralidad de red. Parte de la información procederá de fuentes abiertas y registros administrativos; otra parte requerirá aportaciones reservadas o clasificadas. El producto final debe ser comparable en el tiempo y útil para priorizar decisiones.

La evaluación no debe limitarse a describir riesgos. Para cada exposición prioritaria ha de identificar opciones de respuesta, autoridad responsable, coste, tiempo de implementación y riesgo residual. Diversificación, reservas, modificación contractual, financiación alternativa, protección de conocimiento, cooperación europea o preparación de una respuesta diplomática son medidas diferentes. Vincular el diagnóstico con alternativas convierte el producto en apoyo real a la decisión.

Integración técnica con gobierno de datos y validación humana

La ESN debería exigir un procedimiento estable para integrar evaluaciones producidas por los organismos competentes. Cada entidad conservaría sus competencias, la custodia de la información y la responsabilidad sobre sus análisis. La integración puede descansar en indicadores, tipologías, patrones, escenarios y evaluaciones agregadas. El acceso a información sensible se mantendría dentro de los cauces legalmente previstos.

La tecnología puede mejorar búsqueda, resolución de entidades, eliminación de duplicados, comparación de escenarios y trazabilidad de fuentes. La inteligencia artificial puede asistir esas tareas cuando existan datos adecuados, entornos seguros, controles de acceso, registro de decisiones y validación humana. Su papel debe definirse como apoyo analítico. La atribución, la priorización y la recomendación estratégica siguen requiriendo responsabilidad institucional identificable. La prioridad es una doctrina común y una arquitectura de datos gobernada; una plataforma sin esas condiciones solo automatizaría la fragmentación.

La interoperabilidad no exige una base de datos central. Puede construirse mediante un vocabulario compartido, identificadores comunes, fichas de exposición, criterios de clasificación y mecanismos de consulta federada. Este modelo reduce transferencias innecesarias, permite actualizar la información en su organismo de origen y facilita

auditoría. La calidad dependerá de que cada afirmación conserve fuente, fecha, nivel de confianza y responsable de validación.

Misiones prioritarias vinculadas a la libertad de acción

La estrategia debería concentrar el esfuerzo en un conjunto limitado de misiones. La primera es la protección de cadenas de suministro críticas para defensa, energía, salud, alimentación, telecomunicaciones y transformación digital. La segunda es la seguridad tecnológica y del conocimiento, incluidas inversiones, adquisiciones, movilidad de talento, propiedad intelectual, nube y tecnologías de doble uso. La tercera es la protección integral de infraestructuras críticas, atendiendo a propiedad, financiación, contratos de operación y jurisdicción.

La cuarta misión es el análisis de coerción económica, sanciones y controles de exportación. La quinta abarca la financiación de amenazas estatales, terroristas, criminales y de proliferación, incluidos mecanismos de elusión y redes logísticas. La sexta examina la exposición financiera y contractual en terceros países relevantes para España, con atención a deuda soberana, concesiones, garantías y financiación de infraestructuras. La séptima incorpora estas variables a ejercicios de crisis y defensa para medir tiempos de efecto, reservas y alternativas reales.

La selección anual de prioridades debería combinar impacto potencial, probabilidad, urgencia, dificultad de sustitución y capacidad efectiva de intervención. Este filtro evita que el sistema intente cubrir toda la economía y permite concentrar equipos multidisciplinares en un número manejable de exposiciones. Las prioridades deben revisarse cuando cambien el entorno, los proveedores, la tecnología o la posición financiera.

Una red público-privada estable y territorialmente informada

La ESN debería ordenar un mecanismo permanente con operadores de sectores estratégicos, asociaciones empresariales, entidades financieras, aseguradoras, universidades y centros tecnológicos. Su utilidad dependerá del retorno que ofrezca mediante alertas desclasificadas, tipologías, guías y canales de consulta. Solicitar información sin compartir contexto produce cooperación formal y escasa inteligencia.

La red necesita niveles diferenciados. Algunos intercambios pueden ser abiertos, otros reservados y los más sensibles bilaterales. La participación debe seguir la necesidad de conocer y contar con comunicaciones adecuadas al grado de clasificación. También

conviene articular enlaces territoriales con comunidades autónomas y clústeres productivos. La detección temprana de una adquisición, la desaparición de un proveedor o la presión sobre un centro tecnológico suele producirse cerca del activo.

Las pymes estratégicas deben recibir un tratamiento específico. Algunas dominan nichos de conocimiento, mantenimiento o componentes sin sustituto, pero su capacidad de protección es menor que la de los grandes grupos. El sistema debería facilitar diagnósticos, canales de alerta, formación y acceso a orientación pública sin imponerles cargas desproporcionadas.

La representación empresarial tampoco debería descansar únicamente en grandes organizaciones agregadoras. Para determinadas cadenas será necesario convocar directamente a proveedores especializados, asociaciones sectoriales, aseguradoras, entidades financieras o centros tecnológicos. La geometría variable propuesta para el SIE permite adaptar cada grupo al problema concreto y reducir tanto los conflictos de interés como la exposición innecesaria de información sensible.

Formación y seguridad de la investigación

La formación constituye una infraestructura del sistema. Los perfiles necesarios abarcan inteligencia, finanzas, geografía, economía, derecho, contabilidad, datos, ciberseguridad, ingeniería, comercio y conocimiento sectorial. La Administración necesita lenguaje y métodos comunes; las empresas requieren capacidades para reconocer presiones, proteger información y comunicar señales relevantes; y las universidades deben identificar riesgos sobre proyectos, financiación, propiedad intelectual, movilidad de personal y colaboraciones sensibles.

La experiencia canadiense aconseja combinar orientación pública, evaluación focalizada y apoyo a investigadores. España podría elaborar guías sectoriales, módulos formativos y procedimientos de consulta para universidades y centros tecnológicos, preservando la apertura científica y evitando restricciones generales. La formación debe extenderse a directivos, responsables de seguridad, investigadores y pymes. Sin cultura compartida, la arquitectura formal dependerá de unas pocas personas y perderá continuidad.

El programa formativo debería diferenciar niveles. Un nivel básico aportaría cultura de seguridad económica y criterios de alerta. Un nivel profesional enseñaría análisis de redes societarias, contratos, cadenas de suministro, financiación y tecnología. Un nivel directivo se concentraría en escenarios, toma de decisiones y gestión de crisis. Los

ejercicios conjuntos entre Administración, empresas y universidades servirían para probar lenguaje común, comunicaciones y tiempos de respuesta.

Interoperabilidad, recursos, evaluación y garantías

España debería diseñar esta capacidad dentro de la Unión Europea y en cooperación con la OTAN y socios aliados²⁵. La interoperabilidad exige formatos comparables, ejercicios, intercambio de indicadores y análisis conjunto de escenarios. El enlace con EU INTCEN, OLAF, la EUIPO y su Observatorio, Europol y el EFECC, el EFIPPP, las UIF y AMLA debe establecerse por función, base jurídica y necesidad de conocer. La convergencia puede producir evaluaciones, tipologías y alertas comunes; no justifica fusionar custodias ni hacer circular datos obtenidos para finalidades incompatibles.

El mandato debe asociarse a recursos, perfiles profesionales y una obligación de reporte. El Informe Anual de Seguridad Nacional ofrece un cauce para informar sobre productos elaborados, ejercicios realizados, sectores cubiertos, cooperación y avances del plan de implementación. Los indicadores deben medir mejora en anticipación y respuesta, no solo reuniones o volumen de datos.

Proporcionalidad, precisión, protección de datos, secreto empresarial y separación funcional son principios de diseño. La seguridad económica no debe convertirse en una categoría abierta ni en proteccionismo sin evaluación. El control parlamentario y la revisión periódica deben comprobar que las medidas responden a riesgos definidos, evitan duplicidades y producen una mejora verificable.

La evaluación debería combinar indicadores de actividad y de efecto. Número de productos, ejercicios o participantes permite conocer el esfuerzo, pero no demuestra utilidad. También deben medirse el tiempo de detección, la calidad de las alternativas identificadas, la reducción de exposiciones críticas, la incorporación de alertas a decisiones y el grado de implantación de las medidas acordadas. Una revisión externa periódica puede comprobar que el sistema conserva foco, legalidad y valor añadido.

Conclusiones

La incorporación de la inteligencia económica y financiera a la ESN 2026 se justifica porque mercados, contratos, financiación, tecnología, datos y cadenas de suministro se

25 OTAN (2022), NATO 2022 Strategic Concept. <https://www.nato.int/en/about-us/official-texts-and-resources/strategic-concepts/nato-2022-strategic-concept>

han convertido en canales de poder. Una estrategia que describa ese entorno sin organizar la capacidad para interpretarlo mantendrá la actual distancia entre diagnóstico y decisión.

España no parte de cero. Dispone de antecedentes doctrinales, órganos especializados, supervisores, registros, comunidad de inteligencia y un marco europeo cada vez más desarrollado. La carencia se encuentra en la convergencia. Falta una cadena estable que conecte prioridades políticas, productos analíticos, coordinación, respuesta y evaluación. Recuperar el SIE como arquitectura federada y gradual permite dar continuidad a la propuesta iniciada en 2011 sin invadir competencias ni precipitar un organigrama.

La aportación conjunta de la IE y la FININT puede resumirse en dos mapas. El primero muestra dónde se concentran dependencias, derechos de control, tecnología y puntos de bloqueo. El segundo revela quién financia, intermedia, garantiza, cobra y se beneficia. Superpuestos, permiten discriminar entre una relación económica ordinaria y una vulnerabilidad susceptible de explotación.

La dimensión institucional debe acompañarse de una dimensión cultural. La formación en la Administración, las empresas y las universidades, la atención a pymes estratégicas y la seguridad de la investigación son condiciones de continuidad. También lo son la detección territorial, las comunicaciones seguras y un retorno útil para los actores privados que colaboren.

La arquitectura propuesta evita dos extremos. El primero sería crear una gran estructura central antes de definir productos, competencias y usuarios. El segundo consistiría en confiar de nuevo en una coordinación espontánea entre capacidades dispersas. Un SIE federado, probado por etapas y sometido a evaluación permite construir dirección común sin destruir especialización. Esta arquitectura debe incluir también una dirección centralizada a nivel político con capacidad real de mando y control. La geometría variable y la necesidad de conocer facilitan la participación de cada actor cuando su aportación sea pertinente.

La calidad del sistema dependerá menos del volumen de datos que de su capacidad para formular preguntas correctas, relacionar fuentes y ofrecer alternativas a tiempo. La tecnología puede acelerar esas tareas, pero no sustituye la doctrina, la confianza ni la

responsabilidad. La inteligencia útil termina en una decisión informada y vuelve al sistema en forma de evaluación y nuevos requerimientos.

La oportunidad de 2026 consiste en fijar un mandato verificable. Si la ESN reconoce estas funciones, ordena un plan de implementación del SIE, exige una evaluación nacional de exposición, integra la dimensión financiera en los escenarios de crisis y establece responsables, recursos, garantías e indicadores, habrá dado muchos pasos para minorar la discontinuidad acumulada. Si se limita a reiterar la conexión entre economía, tecnología y seguridad, el diagnóstico será correcto pero la capacidad del Estado permanecerá sin cambios en un entorno cada vez más complejo y disputado.

*Juan Carlos Fernández Cela**
Profesor de la Universidad Complutense de Madrid (UCM)
*Col. (R) José Fuentes García**
Profesor de la ESFAS/CESEDEN