REAL INSTITUTO elcano ROYAL INSTITUTE 25 AÑOS·YEARS

Por una gobernanza ampliada de la ciberseguridad

Félix Arteaga, Javier Alonso

Elcano
Policy Paper

Julio 2026

Real Instituto Elcano

Inteligencia global en español

El Real Instituto Elcano es el *think tank* español líder en estudios internacionales y estratégicos, y un centro de pensamiento de referencia en Europa y en el mundo. Constituido en 2001 como fundación privada de interés general, nuestra misión es contribuir a la elaboración de respuestas innovadoras, rigurosas e independientes sobre los retos globales y su gobernanza, y sobre el papel de España en Europa y en el mundo, al servicio de los decisores públicos y privados, y de la sociedad en su conjunto.

La estructura organizativa del Real Instituto Elcano refleja los principales apoyos públicos y privados que hacen posible su labor y favorece el intercambio de ideas en un entorno plural e independiente. El más alto órgano de gobierno es su Patronato, bajo la presidencia de honor de S.M. el Rey Felipe VI. Dispone además de un Programa de Socios Corporativos.

www.realinstitutoelcano.org

REAL INSTITUTO elcano ROYAL INSTITUTE 25 AÑOS • YEARS

Por una gobernanza ampliada de la ciberseguridad

Félix Arteaga, Javier Alonso

Julio 2026

C/ Príncipe de Vergara, 51
28006 Madrid
www.realinstitutoelcano.org

ISSN 2255-5293
Depósito Legal: M-8692-2013

Índice

Resumen ejecutivo

El avance de la economía digital aumenta el desfase entre el desarrollo de la digitalización y la seguridad de las redes y sistemas de información que la soportan. La complejidad de la ciberseguridad no cesa de aumentar. A las dimensiones operativas y técnicas de seguridad se han ido superponiendo otras geopolíticas, industriales, tecnológicas, diplomáticas o regulatorias que condicionan la eficacia de las anteriores. El modelo de gobernanza vigente responde a un enfoque de seguridad, en el que prima la protección de las infraestructuras críticas y la gestión de incidentes de ciberseguridad sin que su diseño le permita abrirse a un enfoque más amplio de seguridad económica que fomente la autonomía estratégica, la competitividad, la base industrial y tecnológica o la participación social. Tampoco responde a un contexto geopolítico como el actual, con actores estatales detrás de grandes campañas en el ciberespacio, por lo que resulta imprescindible incorporar componentes relevantes de defensa, acción exterior e inteligencia a la gobernanza. El modelo vigente, a pesar de sus logros innegables, da síntomas de insuficiencia. Crece la asimetría entre la gestión de las dimensiones de seguridad y la de las que no lo son. Aumentan los ataques y su impacto sobre los sistemas con protección más deficientes. Crece el desfase entre las obligaciones y los recursos para atenderlas del sector público. Se agranda la asimetría en el reparto de los costes, las obligaciones y las responsabilidades entre los sectores público y privado; la colaboración público-privada retrocede respecto a los niveles de confianza e influencia anteriores.

Este *Policy Paper* no cuestiona la importancia de las dimensiones de seguridad para el modelo de gobernanza actual, pero reivindica la necesidad de equilibrar la atención que se dedica a esas dimensiones con la que se debe dedicar a otras dimensiones postergadas en la gobernanza actual para avanzar hacia un modelo multidimensional y participativo. Sus contenidos se han elaborado mediante discusiones bilaterales y colectivas con los colaboradores públicos y privados del Grupo de Trabajo sobre Ciberpolíticas del Real Instituto Elcano, siendo las recomendaciones aportadas al final del documento de responsabilidad exclusiva de los autores.

1. Introducción. Hacia un modelo de gobernanza de ciberseguridad ampliada

Introducción. Hacia un modelo de gobernanza de ciberseguridad ampliada

La ciberseguridad no es un fin en sí mismo, sino un instrumento necesario para la digitalización y la economía digital. La importancia de la implantación de tecnologías de la información y la comunicación (TIC) para la economía y la productividad se traduce en agendas de digitalización. La ciberseguridad no aparece incorporada hasta la fecha en la digitalización desde el diseño, sino después, cuando los ataques sobre las redes y sistemas de información que la soportan ponen en riesgo la confianza y el avance de la digitalización. En términos temporales y de jerarquía política, las políticas de digitalización preceden sistemáticamente a las de ciberseguridad, tanto en España como en el marco europeo en el que se inscriben. Para reducir el desfase entre la digitalización y la seguridad surge un modelo de gobernanza centrado en la protección de las infraestructuras críticas y en la gestión de incidentes y crisis.

Posteriormente, nuevos fenómenos como la confrontación geopolítica, la guerra híbrida, el COVID-19 o la disrupción tecnológica, principalmente centrada en la inteligencia artificial (IA), han aumentado el desfase entre las dimensiones de seguridad que atiende el modelo de gobernanza y las necesarias para satisfacer las crecientes dimensiones de la digitalización. Debido al incremento exponencial de ciberataques potenciados por la IA, y su inevitabilidad, la ciberseguridad ha pasado a ser un componente más de la resiliencia de los países y de las empresas. Los gestores han tenido que ampliar su enfoque de gestión de riesgos desde el cumplimiento y la prevención a la mitigación de daños y a la recuperación.[1]

Los actores privados, y en particular los que prestan servicios esenciales, han ido añadiendo nuevas dimensiones a su gestión de riesgos a medida que ha avanzado la transformación digital desde la seguridad física a la lógica, a la de cumplimiento normativo o a la geopolítica que afectan a la ciberseguridad. Por el contrario, el modelo vigente de gobernanza continúa enfocado hacia sus dimensiones de seguridad y no se ha abierto a un enfoque más amplio y participativo para potenciar la resiliencia general. Los actores públicos apenas han desarrollado la gestión de las interdependencias entre las nuevas dimensiones y focalizan su gestión en la protección técnica de las redes, sistemas de información y datos, sin asumir e integrar las nuevas dimensiones junto con las tradicionales de ciberseguridad.

Este *Policy Paper* propone el tránsito desde un modelo restringido de gobernanza de la ciberseguridad, centrado en la protección y en la gestión de incidentes de redes, sistemas de información y servicios esenciales, a un modelo de gobernanza más amplio que cubra otras dimensiones

1 Félix Arteaga y Javier Alonso, "La ciberresiliencia, entre la ciberseguridad y la resiliencia", ARI 80/2024, (17/VI/2024).

estrechamente vinculadas a la ciberseguridad como la económica, la industrial y tecnológica, la ciberdefensa, la ciberdiplomacia, la lucha contra la cibercriminalidad, el marco regulatorio, los derechos y libertades fundamentales o la resiliencia, entre otras existentes o que puedan emerger como indica la Figura 1.

Figura 1
Ampliación del modelo de gobernanza

Fuente: elaboración propia

La transformación digital conlleva, por un lado, que la ciberseguridad desborda los silos tradicionales de seguridad (interior, inteligencia, justicia) para hacerse presente en los demás sectores públicos y, por otro, que la gobernanza de la ciberseguridad tiene que abordar nuevas dimensiones y un enfoque intersectorial porque la mera gestión tradicional de riesgos no potencia eficazmente la ciberresiliencia. Tal y como reconoció la Estrategia de Ciberseguridad de la Unión Europea (UE) de 2020, la gobernanza de la ciberseguridad, además de actualizar la Directiva NIS1, debía preocuparse de la ciberdefensa, el espacio, la ciberdiplomacia, las inversiones, el internet de las cosas, el apoyo a las pymes, la agenda contra el ciberdelito, la cooperación al desarrollo o la industria, entre otras.2Al reconocerlo, la UE puso en marcha un modelo de gobernanza ampliada, multidimensional y multinivel que estrecha la interacción de sus diversas políticas e instrumentos con los de ciberseguridad como refleja la Figura 2.

2 Comisión Europea, "EU'sCybersecuritythe Digital Decade, JOIN (2020)18 de 16 de diciembre.

Figura 2

Compendio de políticas asociadas al ecosistema europeo de ciberseguridad (políticas para la ciberseguridad)

Fuente: Christina Ruppp. [3]

En línea con la ampliación propuesta por la UE, la Organización para la Cooperación y el Desarrollo Económico (OCDE) ha adoptado un concepto de *seguridad digital* que se diferencia de la ciberseguridad en que resalta los aspectos sociales y económicos, la protección de los activos, reputación, oportunidades y la continuidad de sus actividades frente a los incidentes que perturban la disponibilidad, integridad y confidencialidad de los sistemas, redes y datos.[4] Para la OCDE, la ciberseguridad es el soporte técnico de las políticas económicas, la regulación de las infraestructuras críticas, la resiliencia y la confianza social en la economía digital.

Las estrategias nacionales de ciberseguridad posteriores han emulado el enfoque multidimensional de la UE y han surgido modelos de gobernanza que centralizan o coordinan las distintas dimensiones. En líneas generales, tienden a superar la división vertical de las dimensiones y reforzar la coordinación entre ellas, bien sea mediante agencias únicas o bajo una autoridad de supervisión distinta de los actores que desarrollan las distintas dimensiones.[5] La centralización o el refuerzo de la coordinación que se reivindica en un modelo de gobernanza ampliada en el sector público no refiere necesariamente a la ejecución (aspectos operativos) sino a la planificación estratégica, la coordinación transversal y la supervisión de las distintas actuaciones. La gobernanza ampliada no elimina la autonomía de ejecución de los actores en cada vertical salvo en aquellos aspectos que mejoran la coherencia y sinergias del modelo, fomentan las economías de escala y la consolidación de redes y ecosistemas.[6]

3 Christina Rupp, “Navigating the EU Cybersecurity Policy Ecosystem”, Interface, (27/VI/2024).

4 OCDE, Policy Framework on Digital Security, 2022. y Global Forum on Digital Security for Prosperity,

5 Robert S. Dewar, “National Cybersecurity and Cyberdefence Policy Snapshots”, CSS-ETH, 2018.

6 Entre otros ejemplos, las redes que fomentan la cooperación público-privada (EuropeanCyber Security Organisation, ECSO), la competitividad (Red de Centros Nacionales de Coordinación, NCCs) o la financiación (Digital EuropePrograme y HorizonEurope).

2. La gobernanza en España

La digitalización arrancó con el Plan Avanza (2005) para acelerar el uso de las tecnologías de información y comunicación (TIC) en empresas, infraestructuras y la Administración (Ley 11/2007).[7] La digitalización masiva continuó con el Plan Avanza 2 (2009) y su Estrategia 2011-2015 que dio paso a la Agenda Digital para España (2013) alineada con la Agenda Digital para Europa (2010).

La ciberseguridad se desarrolló con posterioridad, de forma reactiva y con menor ritmo de crecimiento y presupuestos que la digitalización.[8] La necesidad de proteger a posteriori un entorno hiperdigitalizado acentuó el desfase y aunque se crearon algunos equipos de respuesta a emergencias (CERT) públicos o privados no se contó con una política o estrategia de ciberseguridad autónoma. La situación cambió a partir de las estrategias de Seguridad y de Ciberseguridad Nacional de 2013, revisadas en 2017 y 2019 respectivamente, cuando se articuló un modelo enfocado a la seguridad y poco integrado en la política económica y digital. En 2020 se aceleró la digitalización, entendida ya como política estructural del modelo productivo, con la agenda España Digital 2025 actualizada en 2026 y la ciberseguridad se incorporó ya como un elemento de acompañamiento de la digitalización.

Precisamente por la necesidad de añadir capas de seguridad a un proceso de digitalización que no las contenía por diseño, la gobernanza de la ciberseguridad en España ha adoptado un enfoque de seguridad desde sus inicios. La prioridad del servicio público era la protección frente a los riesgos del ciberespacio, lo que explica la mayoritaria presencia de actores de seguridad en el sistema. En el modelo actual ha primado la seguridad operativa y técnica, a pesar de que han aparecido nuevas dimensiones como la geoestratégica, la económica, la tecnológica o la industrial y de que se ha incrementado la importancia de dimensiones como las de la ciberdefensa, diplomacia, justicia o resiliencia que afectan al rendimiento de las políticas de ciberseguridad.

7 Ley 11/2007 de 22 de junio de acceso electrónico de los ciudadanos a los servicios públicos.

8 El Centro Criptológico Nacional se creó en 2006, el Centro Nacional para la Protección de las Infraestructuras Críticas -luego renombrado como de Infraestructuras y Ciberseguridad, en 2007 y el Mando Conjunto de Ciberdefensa -posteriormente denominado de Ciberespacio- se creó en 2013.

Como resultado, España dispone de un modelo de gobernanza de ciberseguridad desde la Estrategia Nacional de Ciberseguridad (ENC) de 2019 que define sus objetivos, líneas de acción y el modelo de colaboración público-privada de acuerdo con la Ley 36/2015 de Seguridad Nacional y con la Ley 12/2018 de Seguridad de las Redes y Sistemas de Información que traspuso la Directiva NIS1. La Estrategia de Seguridad Nacional (ESN) de 2021, a pesar de que no enunció un concepto amplio de ciberseguridad, incluyó muchas de sus dimensiones, como la competición geopolítica, las tecnologías disruptivas, la gobernanza democrática, la soberanía digital, la protección de los derechos y libertades o el progreso económico, lo que abre el camino a un modelo de gobernanza ampliado en la revisión de la ENC prevista para 2026.[9]

Los avances en la digitalización y el incremento de la inseguridad aconsejaron a la UE reforzar la gobernanza de la ciberseguridad actualizando la Directiva NIS1 mediante la Directiva NIS2 en 2022.10 La trasposición correspondiente se encuentra en proceso de tramitación mediante el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad.11La aprobación por el Consejo de ministros el 14 de enero de 2025 y su posterior consulta pública ha generado un amplio debate entre actores públicos, privados y expertos en ciberseguridad porque introduce cambios en la estructura de gobernanza española con implicaciones para entidades públicas, empresas estratégicas y sectores críticos.

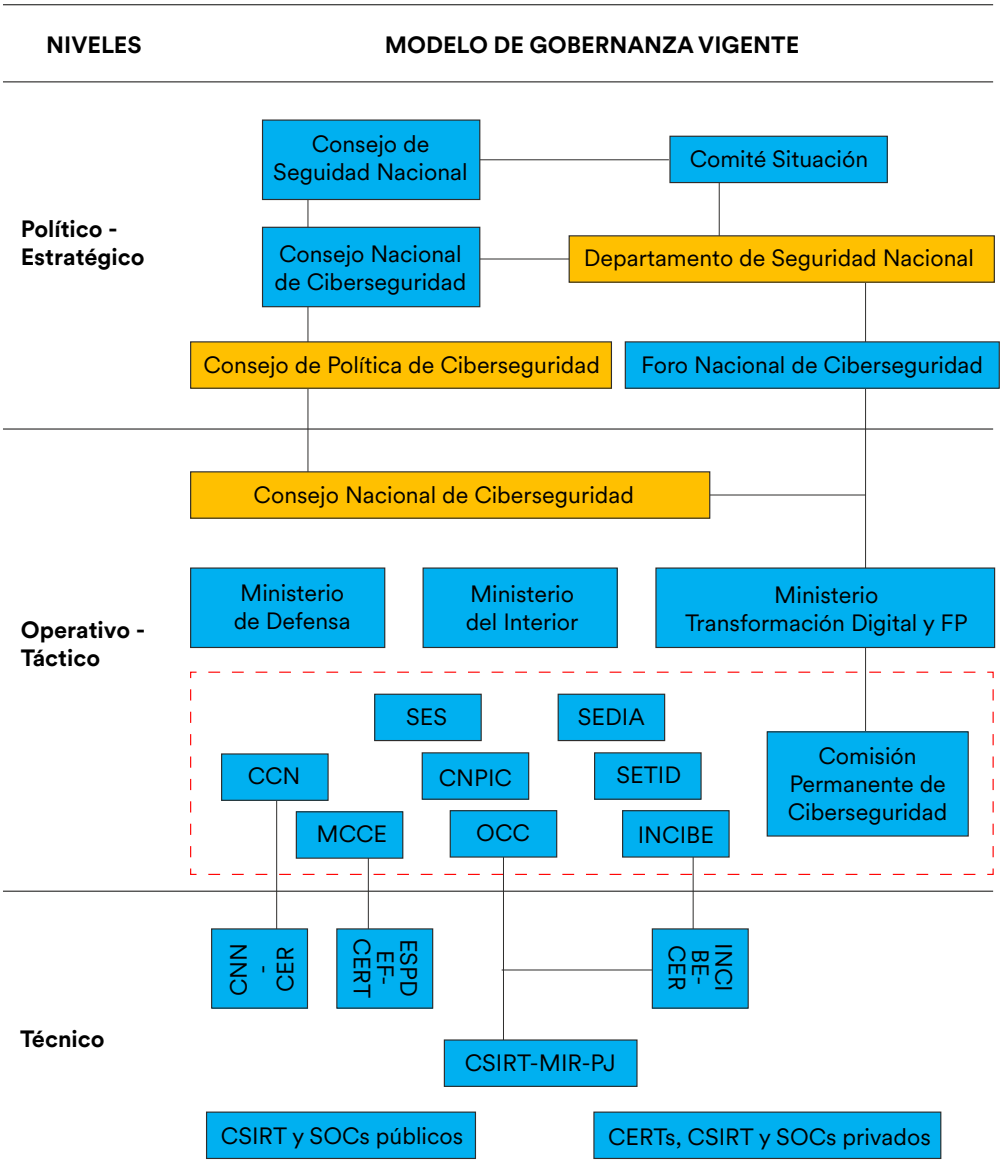
En primer lugar, el Anteproyecto mantiene el enfoque de gobernanza restringida a “todas las actividades necesarias para la protección de las redes y sistemas de información, de los usuarios de tales sistemas y de otras personas afectadas por las ciberamenazas”. Propone definir un marco de gobernanza que aclare las funciones y responsabilidades de las autoridades de control, que sustente la cooperación y la coordinación a nivel nacional, dirigida por el Centro Nacional de Ciberseguridad (CNC) de nueva creación, los CERT nacionales de referencia y los puntos de contacto sectoriales, así como la coordinación y la cooperación entre dichos organismos y las autoridades competentes con arreglo a actos jurídicos sectoriales de la Unión.

9 Ministerio de la Presidencia, Justicia y Relaciones con las Cortes, Orden PJC/522/2025, 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 una nueva Estrategia Nacional de Ciberseguridad.

10 Directiva (UE) 2022/2555 de 14 de diciembre sobre medidas para a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).

11 Ministerio del Interior, Anteproyecto de la Ley de Coordinación y Gobernanza de la Ciberseguridad, (14/I/2025).

Figura 3.
Organigrama del modelo vigente de gobernanza



Fuente: elaboración propia (Pendiente de definición de competencias)

En la Figura 3 se esboza el organigrama de la gobernanza tras la trasposición de la Directiva NIS2 en relación con las políticas de ciberseguridad y la gestión de incidentes. En el modelo predominan los actores de ciberseguridad y públicos sobre los de digitalización y privados. Entre los primeros, destacan los Ministerios de Defensa, Interior y Transformación Digital, sobre el resto de los que participan en el Consejo Nacional de Ciberseguridad. La coordinación interministerial, en una Administración General del Estado fragmentada en silos y con multitud de autoridades competentes, se ha tratado de resolver mediante formatos colegiados y la dinamización estratégica del Departamento de Seguridad Nacional (DSN).

Los grandes actores privados de las infraestructuras críticas se agrupan en torno al Ministerio del Interior (Centro Nacional de Protección de Infraestructuras Críticas, CNPIC, y Oficina de Coordinación de Ciberseguridad, OCC), mientras que los de las tecnologías de la comunicación lo hacen con el Ministerio de Transformación Digital y Función Pública (Secretaría de Estado de Digitalización e Inteligencia Artificial, SEDIA, y el Instituto Nacional de Ciberseguridad, INCIBE). La colaboración público-privada a nivel estratégico se desarrolla en el Foro Nacional de Ciberseguridad mientras que el INCIBE se encarga principalmente de la técnico-operativa.

El Consejo de Seguridad Nacional (CSN) lidera el nivel político-estratégico y, asistido por el Consejo de Ciberseguridad Nacional, establece directrices estratégicas y políticas para la ciberseguridad. El DSN se ha encargado de desarrollar las directrices políticas y estratégicas de ciberseguridad, elaborar el Plan Nacional de Ciberseguridad y coordinar a los distintos actores, así como recabar información de los niveles inferiores en su Célula de Coordinación para elevarla al Comité de Situación en situaciones de crisis. Falta por integrar en este nivel la participación de las Comunidades Autónomas en lo que podría ser un formato colegiado más, tipo Consejo, para coordinar la Política de Ciberseguridad multinivel.

La pluralidad de autoridades competentes en el nivel operativo ha dificultado la gobernanza. El DSN ha tratado de sostener la coordinación, pero no ha contado con el nivel jerárquico ni los recursos necesarios para imponer la coordinación. El Anteproyecto ha creado un nuevo órgano para resolver esta carencia: el Centro Nacional de Ciberseguridad (CNC), pero su naturaleza, estructura, competencias y capacidades no se conocerán hasta su desarrollo reglamentario que tendría lugar un año después de la aprobación de la Ley. La indefinición transitoria de funciones no permite conocer cómo liderará la coordinación y con qué instrumentos contará, una clarificación necesaria porque los actores gubernamentales han rechazado la creación de una Agencia con capacidad de supervisión sobre ellos y, a falta del desarrollo reglamentario, parece que se busca un modelo laso de coordinación.

La actual indefinición no permite conocer la futura redistribución de competencias de coordinación entre el CNC y el DSN, por ejemplo, en relación con la Comisión Permanente de Ciberseguridad, un grupo de trabajo interministerial en el que se coordinan los aspectos operativos y el seguimiento y asesoramiento sobre los riesgos técnicos y operativos para apoyo del Consejo Nacional de Ciberseguridad. En principio, y salvo determinación posterior, parece que el CNC se ubicará en el nivel operativo, sin entrar en la gestión político-estratégica del resto de órganos. Su adscripción al Gabinete de la Presidencia le permitiría asumir en el futuro nuevas funciones, aunque no se sabe si dependerá del director del Gabinete

o de su director adjunto, un nivel inferior del organigrama al que acaba de descender el DSN. El Anteproyecto no establece el rango, carácter y estructura administrativa del CNC, pero da un plazo de doce meses desde su entrada en vigor para definirlas, lo que abre un proceso de prueba y error de al menos un año.

El CNC asumirá el liderazgo de la gestión de crisis de ciberseguridad, incluso a gran escala, mientras que la crisis no derive en una situación de "interés para la seguridad nacional", a gestionar por el Comité de Situación, o en una situación que afecte a la defensa nacional, a gestionar desde el ESPDEF-CERT con apoyo del CCN-CERT e INCIBE-CERT. La gestión de crisis se iniciará con la notificación de incidentes al CNC que evaluará su impacto para asumir su gestión o alertar al Consejo Nacional de Ciberseguridad sobre la evolución de los incidentes con potencial para devenir en crisis de seguridad nacional, como hasta ahora venía haciendo el DSN. Activará los distintos comités sectoriales y gestionará la crisis con planes y recursos propios[12], salvo incidentes que se gestionen en la red europea para crisis de ciberseguridad (EU-CyCLONe).

Los cambios -siempre que se dote a la Administración de recursos suficientes- facilitarán la coordinación técnica y operativa entre los equipos de respuesta a incidentes de referencia nacional (CERT) del Centro Criptológico Nacional (CCN), del Mando Conjunto del Ciberespacio (MCCE) y del Instituto de Ciberseguridad (INCIBE) con los equipos de respuesta a incidentes (CSIRT) y centros de operaciones (SOC) públicos y privados. El Anteproyecto genera dudas, expresadas en las consultas públicas conocidas, sobre la capacidad del CNC para coordinar la multitud de autoridades competentes dispersas por la Administración General del Estado, las Comunidades Autónomas y sectoriales. Sin integración, permanencia, estabilidad de recursos o incentivos presupuestarios, parece difícil que el CNC pueda coordinar eficazmente a los actores públicos del modelo y, más difícil aún, que pueda integrar en el modelo a nuevos actores como las Comunidades Autónomas, entidades locales, sector privado, academia y sociedad civil, por no hablar de nuevas dimensiones.

12 En los incidentes significativos o supuestos de especial gravedad, la coordinación técnica de los CSIRT corresponde al CCN-CERT siguiendo las instrucciones del CNC.

3. La necesaria ampliación de las dimensiones de gobernanza

A pesar de los cambios introducidos por el Anteproyecto, el enfoque de seguridad de la gobernanza de la ciberseguridad no es suficiente para gestionar el perímetro ampliado de la seguridad digital. El Anteproyecto mantiene un modelo de gobernanza centrado en la seguridad a pesar de que introduce tímidamente referencias a la resiliencia, la continuidad de servicios, y la coordinación intersectorial, aunque siguen sin traducirse en una integración real entre la gobernanza con la política industrial, la innovación, el talento o la seguridad económica. Este ya no se reduce a la protección de redes y sistemas de información ni a la gestión de incidentes, sino que se proyecta sobre ámbitos como la economía, la industria, la defensa, la acción exterior, la justicia, la regulación, los derechos y la resiliencia social. El modelo de gobernanza ampliada debe incluir aquellas políticas para la ciberseguridad que aseguran su eficacia en todas las dimensiones del espectro. Las dimensiones que se analizan a continuación deben integrarse como pilares de esa ciberseguridad ampliada que el modelo español aún no ha integrado plenamente en su diseño institucional ni en la distribución efectiva de poder e influencia. Pueden atribuirse a los órganos del nivel político-estratégico de la Figura 3, a pesar delas cautelas formuladas respecto a la marginación de actores que no son de seguridad ya expresada en esos órganos.

3.1. Dimensión económica

La ciberseguridad, la protección de las redes y el uso de los sistemas de información, no son fines en sí mismos, sino medios para que los usuarios y empresas accedan a los servicios que la economía digital y la digitalización les ofrecen. Esto plantea a la gobernanza el dilema de cómo equilibrar la

lógica de la seguridad (resiliencia frente a los ciberataques) con la lógica económica (fomentar el desarrollo del mercado digital). Cada sistema de gobernanza busca un equilibrio entre ambas lógicas que dan como resultado un amplio espectro de enfoques, desde el que busca reducir riesgos de seguridad sin preocuparse por el impacto de la regulación en la economía, al que busca todo lo contrario a través de una regulación más ligera.

Por ejemplo, la Directiva NIS1 de la UE nació como una norma de armonización económica -no de seguridad nacional-, en base al artículo 114 Tratado de Funcionamiento de la UE (mercado interior), que no pretendía "asfixiar" a las empresas con requisitos de seguridad desproporcionados, especialmente a pymes y startups del mercado digital sino crear confianza digital para estimular la economía, con un enfoque mínimo común de seguridad. En su trasposición, cada Estado miembro aplicó su propia lógica de seguridad y económica para frenar la inseguridad o el desarrollo económico. Posteriormente, la Directiva NIS2 mantiene la base legal del mercado interior y sigue siendo un instrumento de seguridad económica, aunque refuerza la dimensión de seguridad (gestión de crisis, coordinación interministerial, protección de infraestructuras críticas) tras constatar que, sin una resiliencia sólida, el mercado digital europeo no puede crecer ni competir globalmente. Pero para ello, la UE tuvo que incluir en su gobernanza instrumentos de consolidación distintos de los estrictamente regulatorios, tal y como reconoce su Estrategia de Seguridad Económica de 2023, que vincula la ciberseguridad a la autonomía estratégica y al control de dependencias críticas.[13]

El desarrollo de la economía digital se ha visto alterado también por las tensiones geopolíticas y las amenazas híbridas que ponen en riesgo las infraestructuras críticas, las cadenas de suministro, la soberanía tecnológica y la privacidad de los usuarios. La preparación para incrementar la resiliencia pública y privada es ahora parte de las agendas nacionales de seguridad y la ciberresiliencia depende de políticas como la industrial, la educación, la tecnología y las inversiones en investigación, desarrollo e innovación.

La dimensión económica se necesita para equilibrar las preocupaciones de seguridad del modelo con las de la competitividad y la autonomía estratégica de las empresas, en las cuentas de resultados y en la continuidad del negocio. Los responsables de la gobernanza deben gestionar riesgos económicos, de suministro, de industria o de talento, muy distintos de la gestión de ciberataques y en sectores estratégicos muy diversos como la energía, el transporte, banca y mercados financieros, sanidad, agua, infraestructuras digitales, servicios tecnológicos, industria nuclear y administración pública. Sus gestores han de estar también atentos al impacto de las inversiones extranjeras en su soberanía tecnológica, a los cambios en las normas europeas de competitividad, a las restricciones proteccionistas y al impacto de tecnologías como la inteligencia artificial.[14]

13 Comisión Europea, "Estrategia europea de seguridad económica", (20/VI/2023).

14 El conflicto geopolítico entre China y los países occidentales ha llevado a la UE a considerar a Huawei y ZTE como suministradores de riesgo. Sin embargo, las medidas a adoptar corresponden a cada país, con la consiguiente inseguridad jurídica y de negocio para sus empresas.

El modelo de gobernanza vigente no cuenta con una dimensión económica por diseño. La Ley 36/2015 de Seguridad Nacional contempla la seguridad económica como una de sus dimensiones, pero no la ha desarrollado mediante una estrategia de segundo nivel. A expensas de que la seguridad económica gane peso en el modelo productivo nacional, el modelo no puede seguir postergando la dimensión económica que afecta principalmente a tres variables: presupuestos, política industrial y competitividad.

La limitación de los recursos humanos, tecnológicos y financieros disponibles afectan a la sostenibilidad del modelo, Por un lado, el sector público no dispone de presupuestos estables ni de mecanismos que adecúen los limitados recursos humanos y técnicos de los que dispone a la creciente carga que les supone la supervisión de las entidades bajo su jurisdicción. Por otro, los sectores privados, y especialmente los públicos, tienen dificultades para reclutar y retener los profesionales cualificados que exige el cambio, lo que afectará al cumplimiento de las obligaciones. La correlación entre los recursos, escasos, y las obligaciones, crecientes, debería llevar a establecer plazos de adaptación razonables, progresivos y asistidos con guías técnicas para facilitar la interpretación y el cumplimiento (operatividad).

Tanto las estrategias, como el plan nacional y los planes sectoriales de ciberseguridad deben acompañarse de planes plurianuales de inversión con medidas de incentivación fiscal y contratación pública innovadora para empresas que desarrollen tecnologías de ciberseguridad certificadas en España o la UE. La ENC vigente se comprometió a potenciar las capacidades humanas y tecnológicas (Objetivo IV) mediante medidas de impulso y dinamización para fortalecer la base industrial, tecnológica y los recursos humanos, pero no se acompañó de los presupuestos o planes específicos.[15] Los recursos son limitados y se dedican más fondos a digitalización que a ciberseguridad. Mientras que el Plan de Recuperación, Transformación y Resiliencia (PRTR) y la Agenda España Digital dedican 17.432 millones a sus planes digitales, de los que sólo han dedicado 1.000 millones de euros al Plan Nacional de Ciberseguridad entre 2022 y 2025 (unos 250 millones al año). En 2025 se presupuestaron 1.157 millones adicionales del Plan Industrial y Tecnológico para la Defensa y Seguridad que no proceden de la digitalización, sino del objetivo de gasto anual en seguridad (1,5% del PIB) acordado en la OTAN.

En conjunto, las inversiones realizadas en ambos presupuestos, digitalización y defensa, en 2025 (1.407 millones de euros) sólo representan aproximadamente el 5% de las partidas de digitalización y de defensa, por lo que se podrían consolidar anualmente estas inversiones, ya fuera en las dos partidas de gasto anteriores o en una partida específica de ciberseguridad similar, entre 1.000 y 1.500 millones de euros anuales.

15 Sólo en mayo de 2025, y al margen de la trasposición, se aprobó un plan de refuerzo para capacidades de ciberseguridad y ciberdefensa de 1.157 millones de euros, el mayor esfuerzo inversor en la historia a distribuir entre los Ministerios de Defensa (60,4%), Transformación Digital y de la Función Pública (22%), e Interior (16,34%).

Recomendación

La ciberseguridad debería contar con una partida presupuestaria que consolidara anualmente un nivel de inversión entre 1.000-1.500 millones de euros para aportar al sector la estabilidad financiera que precisa.

La ENC vigente aspira a potenciar la industria de ciberseguridad y el talento para fortalecer la autonomía digital (Objetivo IV, Línea de Acción 5). La aspiración no se ha traducido en planes ni inversiones concretas para potenciar la base industrial y tecnológica de la ciberseguridad, sino en medidas específicas para fomentar la ciberseguridad y la digitalización de las industrias, que no es lo mismo. En particular, la ciberseguridad industrial OT sigue siendo una asignatura pendiente y gran parte de los actores y sectores industriales carecen de formación en seguridad digital. La autonomía digital es un requisito necesario, pero no suficiente para incrementar la autonomía estratégica, por lo que es necesario adoptar una dimensión industrial y un responsable de esta.[16]

El fomento de la industria y la tecnología de ciberseguridad nacional no aparece como un eje central de la gobernanza actual ni ésta aboga por políticas y planes de desarrollo específicos.17Su atención primaria es la protección de las redes y sistemas y aspectos como la autonomía estratégica o el desarrollo de ecosistemas industriales y tecnológicos competitivos excede a su agenda de trabajo. La reducción de la dependencia tecnológica de terceros debe enmarcarse en las políticas de digitalización, industria y seguridad económica, por lo que su liderazgo intergubernamental debería corresponder al Ministerio de Transformación Digital y Función Pública, en colaboración con los Ministerios de Industria, Educación y Ciencia e Innovación para aprovechar su tracción público-privada en materia industrial.

La gobernanza debería ocuparse de la disrupción tecnológica en curso porque afecta a la soberanía estratégica en la medida que la inteligencia artificial, la virtualización de plataformas IT con un modelo de fuentes abiertas (Open Source), la computación cuántica o las neurotecnologías alteran los parámetros de definición de las normas. También potencian la competitividad del sector privado. Los reguladores pertenecen al sector público y, por tanto, no se ven afectados directamente por el coste de las medidas que adoptan porque la gobernanza actual traslada ese coste a los regulados públicos y privados. El sector público se ha limitado a regular los aspectos operativos y técnicos de la ciberseguridad sin contemplar la dimensión industrial o de negocio, salvo las que se mencionan a

16 En el nivel estratégico de la Figura 3 no aparece ningún miembro responsable de la dimensión industrial y tecnológica y el Anteproyecto no asigna a los responsables del nivel operativo liderar la política industrial, coordinar la I+D+i ni fomentar la autonomía estratégica.

17 Salvo para la coordinación de la participación nacional en el Centro Europeo de Competencia Industrial (INCIBE). El Foro Nacional de Ciberseguridad dispone de dos grupos de trabajo sobre industria e innovación, civil y militar.

continuación en relación con el INCIBE. Cada autoridad reguladora añade capas adicionales de seguridad sin tener en cuenta su impacto sobre el cumplimiento normativo y la cuenta de resultados de los regulados.[18]

Dentro del modelo actual, la gestión industrial corresponde al INCIBE por defecto ya que es el único actor con experiencia para impulsar el ecosistema empresarial y tecnológico, fortalecer su resiliencia y capacitación y conectarlo con otros ecosistemas internacionales dentro de su plan estratégico 2021-2025.[19] A este impulso debe añadirse el de las Comunidades Autónomas que comienzan a desarrollar sus propios ecosistemas en colaboración con INCIBE y los corredores tecnológicos del Ministerio de Defensa.

En este sentido, la SEDIA, el INCIBE y las Comunidades Autónomas gestionan el programa piloto ACTIVA Ciberseguridad, dentro de la Estrategia de Industria Conectada 4.0, y financiado con fondos del Mecanismo de Recuperación y Resiliencia del Ministerio de Industria y Turismo.20 Un programa similar con mayor ambición -un PERTE de ciberseguridad- podría integrar las capacidades industriales y tecnológicas dispersas para generar sinergias, ganar escala y autonomía estratégica. La aprobación de un PERTE reforzaría la naturaleza estratégica del sector tecnológico e industrial de la ciberseguridad para la digitalización.

Recomendación

> Adoptar un PERTE que permita integrar la base industrial y tecnológica de la ciberseguridad y la ciberdefensa en una política industrial a largo plazo que fomente la soberanía estratégica mediante la colaboración público-privada.

3.2. Dimensión de ciberdefensa

La ciberdefensa constituye otra dimensión específica de la ciberseguridad ampliada, con un sistema propio que en España sigue separado del resto a pesar de que las amenazas híbridas y la convergencia civil-militar en el ciberespacio desdibujan esa separación. Ésta tenía sentido cuando los incidentes afectaban a intereses privados, pero ahora los ciberataques se dirigen contra actores privados para socavar su contribución a la resiliencia general. La evolución de la política europea de ciberdefensa, la apuesta por redes de CERT militares interconectadas y la noción de “ciberpostura”

18 Asimismo, el sector tecnológico se ve afectado por el Reglamento Cyber Resilience Actque va a exigir delinear las competencias de ejecución en España y que debería formar parte activa en su desarrollo regulatorio.

19 De los aproximadamente 72.000 millones de euros de fondos NextGeneration destinados a España, una tercera parte se ha destinado a digitalización. INCIBE dedicó 564 millones de fondos PRTR a sus actividades junto a 69 de su presupuesto ordinario en 2025.

20 Secretaría General de Industria y de la PYME, Programa ACTIVA Ciberseguridad

refuerzan la necesidad de un enfoque integrado. Desde una lógica de ciberseguridad ampliada, la ciberdefensa no puede abordarse solo como un subsistema especializado. La ESN debería reforzar su función de apoyo a los sectores público y privado de la ciberseguridad y aclarar el marco de uso de capacidades de defensa activa y disuasión.

En España, la ciberdefensa ocupa un espacio propio del sistema de ciberseguridad. Tanto la Ley 8/2011 de protección de infraestructuras críticas como los RDL 12/2018 y 43/2021 de trasposición de la NIS posteriores excluyen las infraestructuras de defensa de su aplicación, lo que marca una separación formal entre la ciberdefensa y la ciberseguridad. No obstante, la Ley de Seguridad Nacional establece el deber de colaboración de las entidades privadas con las Administraciones Públicas cuando afecte a la seguridad nacional (art. 7.1). En la misma línea, el RDL 12/2018 asignó al ESPDEF-CERT la colaboración con el resto de los CERT nacionales y con los operadores que tengan incidencia en la defensa nacional siempre que se determinen reglamentariamente (art. 11.3) lo que pone de relieve su potencial de convergencia, aunque cada componente preserve su autonomía operativa.

El Anteproyecto también aboga por articular mecanismos de apoyo, coordinación e intercambios con entidades y operadores que inciden en la defensa nacional (proveedores de bienes y servicios necesarios), pero excluye de su ámbito de aplicación a las entidades de la Administración pública implicados en la defensa, quedando las entidades privadas con incidencia en ella bajo control militar (Ministerio, Estado Mayor de la Defensa, Mando Conjunto del Ciberespacio y ESPDEF-CERT).

La Estrategia Europea de Ciberseguridad de 2020 incluyó medidas destinadas a impulsar las capacidades de ciberdefensa de la UE tras la consolidación del ciberespacio como un dominio más de las operaciones militares. La Estrategia reivindicó una mayor cooperación entre las comunidades de ciberseguridad y las de ciberdefensa, poniendo en marcha una red de CERT militares interconectados (el ciberescudo). La UE ha seguido apoyando la colaboración en su "ciberpostura" de 2022[21], en la política de ciberdefensa de noviembre de 202222 y en la Estrategia de Preparación de 202523.

La colaboración entre el sector privado de la ciberseguridad y el público de la defensa ha aumentado su importancia en un entorno estratégico de amenazas híbridas dirigidas por igual a objetivos civiles y militares. La colaboración solapa intereses públicos y privados, especialmente los

21 Consejo Europeo, Doc. 9364/22 de 23 de mayo sobre conclusiones para el desarrollo de una ciberpostura de la UE.

22 JOIN (2022) 49 de 10 de noviembre sobre "Política de Ciberdefensa de la UE" y conclusiones del Consejo sobre la misma 9618/23 de 22 de mayo.

23 Alto Representante, JOIN (2025) 130 de 26 de marzo sobre la estrategia de preparación de la UE.

asociados a la soberanía tecnológica e industrial del país que precisan un ecosistema industrial (hub) para desarrollar capacidades operativas de ciberdefensa. Estas capacidades deben servir también para proteger las infraestructuras digitales porque estás no sólo son vitales para la defensa, sino también para la resiliencia nacional.[24] De hecho, la propia OTAN ha establecido el objetivo de inversión en su seguridad en el 1,5% del PIB, una decisión que permitiría a España destinar presupuestos de defensa a partidas de ciberdefensa, ciberseguridad y resiliencia.

La ENC vigente marcó el paso de un modelo de gobernanza preventivo y defensivo a otro con "elementos de mayor fuerza disuasoria", lo que requería disponer de medidas disuasorias en una zona intermedia entre la ciberseguridad y la ciberdefensa, en la que actores públicos y privados puedan compartir instrumentos disuasorios contra las ciberamenazas según establezca su regulación. Reconoció la necesidad de que la defensa de ciudadanos, autónomos y empresas fuera "más allá de las medidas de autoprotección que ellos pueden tomar" y propuso implantar medidas de ciberdefensa activa. Estas siguen sin implantación y sin que se defina el propio concepto de ciberdefensa activa. Mientras que la ENC emplea el término de ciberdefensa activa para referirse a la protección de ciudadanos y empresas (Objetivo III, Línea de Acción 1), las Fuerzas Armadas reivindican ese término de ciberdefensa activa para las operaciones militares y prefieren emplear el término de ciberprotección activa para denominar las actuaciones civiles.

Por el contrario, en la ciberseguridad civil se utiliza con profusión la denominación de defensa o ciberdefensa activa para referirse a algunas capacidades más agresivas que las habituales de protección. Incluso, el sector público (CCN-CERT) ha desarrollado algunas medidas denominas de ciberdefensa activa que se encuentran a disposición del sector privado, pero sin un marco regulador de su uso y dentro del paradigma defensivo.[25] Para ser legales y eficaces, las medidas de ciberdefensa activa precisan que se regule su concepto, empleo y atribución de responsabilidades (quién debe hacer qué).

La lógica de la cooperación público-privada para la protección redes y sistemas críticos ha cambiado radicalmente. En el actual contexto de los conflictos híbridos, donde actores paraestatales promovidos por Rusia o China atacan las empresas privadas a través del ciberespacio, no por su condición privada sino por su importancia para la economía y seguridad nacional, la protección ante incidentes no es un asunto particular de las víctimas sino del Estado. La defensa de los intereses nacionales en riesgo corresponde al Estado, pero este desplaza la mayor parte del coste y la responsabilidad de la protección a los actores privados, principalmente a los proveedores de servicios esenciales y operadores deinfraestructuras críticas.

24 Paolo Grassia, "Europe's defence starts with networks, and we are running out of time", Politico, (2/XII/2025)..

25 BasqueCyberSecurity Center, "Defensa activa", incluyen direcciones de correo falsas, archivos ejecutables falsos, balizas, claves AWS falsas y otros.

El modelo de gobernanza vigente mantiene a un sector público como la ciberdefensa, que ostenta el monopolio de la disuasión, al margen de la protección cotidiana al sector privado. Este nuevo campo de batalla exige al sector privado la dedicación de recursos económicos y humanos que suponen una carga enorme en detrimento de la competitividad de las empresas. El marco de actuación de la ciberdefensa, y a falta de regulación de la defensa activa, es reactivo, limitado e insuficiente. Ni se asegura protección al sector privado ni se les habilita para ejercer capacidades de autodefensa debidamente regladas.

Finalmente, la gobernanza no puede permitirse el lujo de seguir sin declarar su voluntad de usar y desarrollar capacidades ofensivas disuasorias ni de reglar el uso de los instrumentos de ciberdefensa activa.[26] La revisión de la ENC debería integrar la ciberdefensa en la gobernanza para subrayar su importancia, reforzar la colaboración entre el sector privado de la ciberseguridad (industrias) y el público de la ciberdefensa (MCCE) para evitar que la oferta tecnológica nacional desaparezca o devenga incapaz de proporcionar capacidades estratégicas críticas para ambos sectores. También, para generar sinergias y fomentar el trasvase de las lecciones aprendidas por el sector de la ciberdefensa en simulaciones y ejercicios avanzados a los responsables privados de la gestión de incidentes.

Por último, la revisión de la ENC debería reforzar la convergencia entre las bases industriales y tecnológicas de ciberseguridad y ciberdefensa. Este encaje es fundamental para asegurar las sinergias entre el desarrollo de las capacidades militares y civiles y aumentar la escala y competitividad de la industria nacional. No todas las dependencias tecnologías de terceros afectan a la ciberseguridad de la misma forma, por lo que la autonomía estratégica debe discriminar entre el nivel de protección a cada sector. Mientras que el nivel de seguridad de las redes civiles permite una mayor penetración de tecnologías extranjeras, sean chinas o estadounidenses, ésta no es habitualmente deseable en áreas tan sensibles como la ciberdefensa donde se debe aspirar al mayor grado de autonomía estratégica posible. Para generar sinergias entre la ciberdefensa y la industria, la política industrial de ciberseguridad debería incluir un hub con un núcleo restringido de industrias nacionales estratégicas y planes plurianuales de inversión para satisfacer las necesidades de las operaciones en el ciberespacio (los fondos asignados dentro del Plan Industrial y Tecnológico de abril de 2025 representan un avance, pero no aseguran su sostenibilidad en el tiempo).

26 Félix Arteaga y Javier Alonso, “El concepto de Ciberdefensa Activa”, ARI 18/2025, (06/II/2025).

Recomendaciones

La Estrategia de Seguridad Nacional debe definir el concepto de ciberdefensa activa, diferenciar el ámbito civil del militar y regular el uso de los instrumentos ofensivos y defensivos.

Las capacidades de ciberdefensa precisan una base industrial y tecnológica (hub) que asegure el máximo nivel de autonomía estratégica posible en la defensa nacional y que, a su vez, retroalimente las capacidades civiles de ciberseguridad.

3.3. Dimensión de ciberdiplomacia

La ciberdiplomacia es una dimensión por construir dentro de la diplomacia digital de la acción exterior española, tiene por función coordinar la gobernanza internacional multilateral con la gobernanza doméstica en materias como defensa, industria, cooperación penal y judicial.[27] Ésta se entiende como el ejercicio de la acción diplomática tanto en ámbitos estratégicos específicos del sector tecnológico como en el uso de herramientas y canales de comunicación digitales para desarrollar la acción diplomática en general. Sin embargo, mientras que el enfoque de diplomacia pública se asocia al uso de los medios digitales, la acción diplomática en relación con la regulación internacional de los usos y medios tecnológicos –la ciberdiplomacia- sigue pendiente de definición en el sistema español de gobernanza.

Por el contrario, la UE ha acuñado ese término para referirse a la diplomacia del ciberespacio[28] que integra las distintas áreas de negociación internacional y desde 2017 ha desarrollado un catálogo de medidas diplomáticas (EU Cyber Diplomacy Toolbox) -a las que contribuye España- que permite graduar la adopción de respuestas diplomáticas conjuntas incluyendo medidas preventivas y sanciones para responder a los ciberataques de terceros.[29]

Las estrategias nacionales de Ciberseguridad y de Acción Exterior han reconocido la importancia de la gobernanza internacional del ciberespacio, pero lo han hecho con formulaciones voluntaristas y sin dotar al Ministerio

27 Secrétariat general de la défense et de la securité nationale. “National Cybersecurity Strategy 2026-2030”, p. 24, (4/II/2026).

28 Andrea Salvi, Heli Tiirmaa-Klaar y James Andre Lewis, “A Handbook for the Practice of Cyber Diplomacy”, EU Cyber Direct.

29 Consejo Europeo, doc. 7299/19 de 14 de mayo sobre medidas restrictivas contra los ciberataques que amenacen a la UE o sus estados miembros.

de los necesarios recursos, prioridades y estructuras. La ENC vigente incluyó la seguridad del ciberespacio en el ámbito internacional (Objetivo V) entre sus finalidades. La regulación internacional del ciberespacio, tanto en su dimensión europea como la internacional, la participación en foros multilaterales, así como el desarrollo de la ciberseguridad como un instrumento de la acción exterior del Estado conforman el núcleo de la ciberdiplomacia. Las medidas que la Estrategia estableció para alcanzar esos objetivos tenían un carácter voluntarista (potenciar la presencia, promover consensos, participar activamente o fomentar el diálogo…) sin desarrollar el concepto y la estructura de ciberdiplomacia necesaria para ello. Las estrategias posteriores de acción exterior han continuado ese bajo perfil de compromiso. La de 2021-2024 reiteraba la voluntad de cooperar a la seguridad y estabilidad del ciberespacio global[30] y la de 2025-2028[31] tampoco señala otras acciones específicas que impulsar el liderazgo internacional en organismos internacionales como la Unión Internacional de Telecomunicaciones, promover acuerdos de cooperación con socios y aliados, especialmente en Sudamérica, o implementar la futura ENC.[32]

Lo anterior revela una debilidad en la estructura de gobernanza, porque no se pueden contribuir a la gobernanza internacional del ciberespacio sin que la acción exterior del Estado cuente con los recursos y prioridades adecuadas en el plano nacional. La ciberseguridad ha contado con escasos recursos diplomáticos para seguir la multiplicación exponencial de foros, iniciativas, sanciones y regulaciones.[33] Además, sus representantes han tenido que compaginar la atención a la ciberseguridad con la de las amenazas híbridas y las propias de la transformación digital, con lo que la ciberdiplomacia carece del concepto y la relevancia que precisaría la acción exterior.

A pesar de las condiciones descritas, el Ministerio compagina su participación en el Consejo Nacional de Ciberseguridad con la coordinación de las relaciones con terceros. Un aspecto importante de éstas es el de la atribución pública de ciberataques como parte de los instrumentos nacionales o europeos de disuasión. En el contexto geopolítico actual, la atribución de ciberataques es un instrumento disuasorio que precisa un aparato de comunicación estratégica especializado para que la atribución produzca efectos ante terceros. Para ello es indispensable que la ciberdiplomacia se coordine con la Presidencia del Gobierno para

30 Ministerio de Asuntos Exteriores, Unión Europea y Cooperación, “Estrategia de Acción Exterior 2021-2024”, (28/I/2021).

31 Ministerio de Asuntos Exteriores, Unión Europea y Cooperación, “Estrategia de Acción Exterior 2025-2028”, (28/I/2021).

32 España aprobó la declaración del Consejo sobre la aplicación del Derecho Internacional al ciberespacio de 24 de noviembre de 2024 para fomentar la cooperación europea e internacional, un compromiso al que ayudaría el desarrollo de la ciberdiplomacia.

33 Entre otros, España participa en el Grupo de Expertos Gubernamentales (GGE) sobre normas de comportamiento responsable en el ciberespacio y en elOpen-Ended Working Group (OEWG) en ciberseguridad, ambos de NN.UU., en la ciberdiplomacia de la UE, en las medidas de confianza de la OSCE y el Consejo de Europa y en Convenio de Budapest sobre ciberdelincuencia.

asegurar la coherencia de la comunicación estratégica. Del mismo modo, decisiones como las del Consejo de Telecomunicaciones de la UE precisarían una participación más proactiva de la ciberdiplomacia nacional en su seguimiento.

Otro ámbito donde la ciberdiplomacia podría contribuir a las políticas para la ciberseguridad es el de la coordinación intergubernamental de los asuntos regulatorios y estratégicos de la ciberseguridad desde la Representación Permanente de Bruselas. Las tareas de coordinación que llevan a cabo los representantes diplomáticos con los representantes de los distintos Ministerios en los procesos de negociación del Grupo de Trabajo Horizontal de Asuntos de Ciberseguridad en Bruselas deberían tener mayor continuidad y apoyo en Madrid para reforzar la sinergia intergubernamental entre representantes y representados

En un sistema de gobernanza ampliada, la ciberdiplomacia debería contar con un concepto y una estructura diplomática con capacidad para atender sus compromisos internacionales en materia de regulación, así como los asociados a la política exterior en el desempeño de la ciberseguridad, la ciberdefensa y las amenazas híbridas. Integrar la ciberdiplomacia en la futura ENC subrayaría su importancia. Sin ello, la contribución de España a la gobernanza internacional del ciberespacio y el perfil de Exteriores en la gobernanza interna de la ciberseguridad seguirán estando por debajo de lo que corresponde a su nivel institucional y a sus intereses estratégicos.

Recomendaciones

La Estrategia Nacional de Ciberseguridad debe recoger el concepto y función de la ciberdiplomacia para la consecución de sus objetivos en materia de regulación internacional del ciberespacio.

La estructura del Ministerio de Asuntos Exteriores debe adecuar sus recursos al protagonismo que la ciberdiplomacia debe asumir en la gestión internacional y doméstica de las políticas para la ciberseguridad.

3.4. Dimensión de lucha contra la cibercriminalidad

La cibercriminalidad se sitúa en la intersección entre la ciberseguridad operativa, la justicia penal, la cooperación policial internacional y la protección de derechos. La cibercriminalidad no sólo afecta a la seguridad de las redes y sistemas de información, sino a la confianza de los usuarios en la economía digital, a su patrimonio digital, a su privacidad y a las libertades y derechos fundamentales de los usuarios. Según datos de Interior, los delitos informáticos que conoce han crecido desde 2019, son numerosos (472.125 en 2023, 26% más que en 2022[34]) y también ha crecido su porcentaje en el conjunto total de delitos (del 9,9% al 19,2%).[35] Las víctimas se enfrentan a la gravosa tramitación de las denuncias y a las limitadas expectativas de resarcimiento, lo que aumenta su renuencia al uso de los servicios digitales. Es, por tanto, una dimensión que recae principalmente dentro de la seguridad interior y su objetivo consiste en prevenir el uso el uso ilícito del ciberespacio (fraudes, contenidos ilegales, material de abuso sexual infantil, delitos como servicio y otros) así como mejorar la capacidad de actuación judicial y policial ante actividades ilícitas a través del ciberespacio (acceso a evidencias, retención de datos y comunicaciones, descifrado).

A diferencia del Ministerio del Interior, que desempeña un papel activo en la protección de las infraestructuras críticas, y de los cuerpos policiales que cooperan con la Fiscalía de Criminalidad Informática, el Ministerio de Justicia apenas contribuye a una dimensión crítica para la ciberseguridad. En la ESN de 2021 figura como objetivo la lucha contra el crimen organizado y la delincuencia grave, pero no incluye las actividades relacionadas con la cibercriminalidad, omisión que debería evitarse en su futura actualización.[36] La ENC vigente sí que define la cibercriminalidad y ha establecido varias medidas para asegurar el uso seguro y fiable del ciberespacio frente a su uso ilícito o malicioso (Objetivo II, Línea de Acción 3).[37] Entre ellas, el Plan Estratégico contra la Cibercriminalidad del Ministerio del Interior de 2021, que ha sido la hoja de ruta para la prevención, cooperación, dotación de capacidades técnicas y mejoras en I+D+i así como de formación en las

34 Sin embargo, el valor acumulado en 2024 correspondiente al cuarto trimestre es de 465.838 delitos informáticos, lo que muestra una disminución de 6.287 delitos con respecto a 2023 (-1.35%).

35 De los 97.348 incidentes de 2024, el 67,6% afectaron a la ciudadanía y el 32,4 a empresa se según el "Balance de Ciberseguridad de INCIBE" en 2024, (26/III/2025). Secretaría Estado Seguridad, Informe sobre cibercriminalidad 2023, p.18.

36 Si que aparece en la Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave de 2025. Orden PJC/864/2025 de 9 de julio,

37 Criminalidad es "el conjunto de actividades ilícitas cometidas en el ciberespacio que tienen por objeto los elementos, sistemas informáticos o cualesquiera otros bienes jurídicos, siempre que en su planificación, desarrollo y ejecución resulte determinante la utilización de herramientas tecnológicas; en función de la naturaleza del hecho punible en sí, de la autoría, de su motivación, o de los daños infligidos, se podrá hablar así de ciberterrorismo, de ciberdelito, o en su caso, de hacktivismo".

Fuerzas y Cuerpos de Seguridad del Estado.[38] Se ha reforzado la Oficina de Coordinación de Ciberseguridad (OCC) que cuenta con un Observatorio que recopila y procesa inteligencia y con un centro de respuesta a incidentes informáticos (CSIRT-MIR-PJ) que apoya las investigaciones policiales y judiciales[39]. El Plan impulsa la coordinación nacional e internacional (cooperación reforzada con EUROPOL, INTERPOL, EUCTF y J-CAT), para el intercambio de inteligencia y la participación conjunta en operaciones y grupos de trabajo.[40]

Desde el punto de vista de la gobernanza, la Administración de Justicia no puede seguir teniendo un papel marginal porque resulta imprescindible la actualización de algunas de las herramientas legales necesarias para la combatir la ciberdelincuencia, tanto en los aspectos penales sustantivos como en los relativos a las herramientas de investigación criminal. En relación con el primer aspecto, sería conveniente la incorporación como delitos en nuestra normativa interna de determinadas conductas que se están detectando con frecuencia en el entorno virtual y que, por el momento, no tienen adecuada respuesta en nuestro Código Penal. Tal es el caso, por ejemplo, del empleo no autorizado de herramientas electrónicas de geolocalización con el objetivo de vigilar electrónicamente a personas concretas y de esa forma atentar contra su intimidad[41] o, también, la tipificación penal como delito autónomo de la suplantación de identidad, tanto de personas físicas como jurídicas, decisión legislativa que ya se ha adoptado en países de nuestro entorno, como Francia, y que en la actualidad es todavía más necesaria dadas las facilidades que ofrece la inteligencia artificial para ese tipo de acciones.

Igualmente preocupa el incremento de las actividades delictivas definidas genéricamente como “crimen como servicio” (crime as a service, CAAS), cuya investigación y persecución penal requeriría la redefinición de algunos tipos penales, particularmente los que sancionan determinados actos preparatorios, para otorgarles una mayor amplitud a fin de que sean de aplicación a la generalidad de las conductas delictivas que se ven facilitadas por esta modalidad delictiva, así como una respuesta penal más grave y acorde con la verdadera entidad de estos comportamientos. En el mismo sentido, sería conveniente revisar alguna de las herramientas de investigación a fin de mejorar la capacidad de actuación, sin menoscabo de las garantías procesales, como cuando se intervienen los servidores utilizados para la prestación de servicios criminales desde la web profunda.

38 Secretaría de Estado de Seguridad, Plan Estratégico contra la Cibercriminalidad, Oficina de Coordinación de Ciberseguridad, febrero 2021.

39 En relación con ello se ha consolidado un canal permanente de comunicación entre la OCC, la Fiscalía y las Fuerzas y Cuerpos de Seguridad del Estado para el traslado de información sobre incidentes de seguridad que presenten indicios de delito. Dicha comunicación tiene su fundamento legal en el art 14.3 del Real Decreto- Ley 12/2018 de 7 de septiembre

40 Secretaria de Estado de Seguridad, Informe de cibercriminalidad 2023, D.G. de Coordinación y Estudios.

41 En relación con esta conducta ha de tenerse en cuenta que la implementación del art. 6 de la Directiva UE 2024/1385 supondrá la regulación de las conductas de ciberacecho en nuestra legislación penal sustantiva.

Resulta imprescindible el registro y tratamiento unificado de las denuncias por parte de los distintos cuerpos policiales nacionales y autonómicos, a partir de bases de datos y parámetros comunes que permitan interrelacionar la información que ofrecen las víctimas de los delitos en línea en las denuncias presentadas, sea cual sea el cuerpo policial receptor. El tratamiento aislado de estas denuncias en relación con actividades delictivas, que por su naturaleza en línea pueden producir efectos en diversos lugares del territorio nacional, está generando graves disfunciones en la posibilidad de perseguir y sancionar de forma efectiva muchos de los ciberdelitos. Como también seria de interés, con ocasión de la transposición de la Directiva NIS 2, un reforzamiento de los canales de comunicación ya establecidos en la actual normativa para que desde los CSIRT -o en su caso desde la OCC- se traslade a los órganos de la jurisdicción penal la información sobre incidentes de seguridad que presenten indicios de delito.

Otro aspecto que requiere de una especial atención es el establecimiento de normativa y protocolos adecuados para la custodia, almacenamiento y, en su caso, realización de los criptoactivos, dada la ausencia de regulación específica al respecto pese a la frecuencia con la que se incautan activos de esta naturaleza cuando se investigan conductas delictivas en línea. Particularmente es de especial interés definir reglamentaria o legalmente la entidad u organismo encargado del almacenamiento y custodia de dichos activos desde su incautación hasta que exista una resolución judicial definitiva sobre el destino de estos.

Asimismo, resulta ineludible y debiera impulsarse prioritariamente la adaptación de la normativa interna a los instrumentos internacionales recientemente elaborados para facilitar la obtención transnacional de evidencias electrónicas con fines de investigación criminal. Nos referimos concretamente al paquete “e-evidence” -Reglamento (UE) 2023/1543 y Directiva (UE) 2023/1544)[42]- y al Segundo Protocolo Adicional a la Convención de Budapest, el primero de ellos orientado a facilitar la conservación y entrega de evidencias electrónicas en el marco comunitario y el segundo con el mismo objetivo, pero con un marco de aplicación territorial más amplio, que resultara de especial utilidad en las investigaciones comunes con las autoridades policiales y judiciales de los países de habla hispana.

Finalmente preocupa la implantación masiva de tecnologías que pueden afectar a la eficacia de la investigación criminal, entre otras, el uso generalizado del cifrado de extremo a extremo en las comunicaciones de las plataformas (WhatsApp, Telegram), la virtualización de las infraestructuras de red de telecomunicaciones o la nueva arquitectura de la red 5G, que dificulta la identificación del operador que genera el tráfico en roaming a

42 Reglamento (UE) 2023/1543 de 12 de julio sobre órdenes europeas de producción y conservación de pruebas electrónicas. Directiva (UE) 2023/1544 de 12 de julio sobre designación de establecimientos y responsables legales para recabar pruebas electrónicas.

efectos de la interceptación de comunicaciones. Estas dificultades se han visto acentuadas con el impacto de la normativa y la doctrina del Tribunal de Justicia de la Unión Europea sobre protección de datos de carácter personal, ya que imponen fuertes limitaciones al almacenamiento y utilización de información de esa naturaleza con fines de investigación criminal y, en consecuencia, determinan la necesidad de adecuación de la Ley 25/2007 a estas nuevas situaciones.[43]

En una gobernanza ampliada, el planteamiento en materia de ciberseguridad debiera preocuparse de prevenir con suficiente anticipación conceptual (alcance, impacto) y temporal que los cambios normativos o tecnológicos no dificulten el acceso de las investigaciones judiciales a las plataformas de internet y a los operadores de comunicaciones electrónicas para pedir datos y contenidos o su retirada. Se debe cohonestar la ineludible obligación de proteger la privacidad, la intimidad y los derechos de las personas con la necesidad de investigar los delitos y poder actuar de forma efectiva frente a una criminalidad cada vez más peligrosa y que también pone en riesgo los derechos y libertades de las personas, una dimensión relevante para la confianza social en la digitalización que debería cobrar protagonismo en la gobernanza.

Recomendación

> La futura Estrategia de Ciberseguridad debería reivindicar un papel más activo a la Administración de Justicia para apoyar a la Fiscalía y cuerpos policiales en su lucha contra la cibercriminalidad, para evitar que el desfase entre las conductas criminales y la respuesta procesal y penal se agrave con los cambios tecnológicos en curso y ponga en riesgo las investigaciones criminales y la confianza social en la digitalización.

43 Ley 25/2007 de 18 de octubre sobre la conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

4. Insuficiencia del modelo de gobernanza

La evaluación del modelo de gobernanza lleva, inevitablemente, a reflexionar sobre si el modelo puede mantenerse con cambios como los anunciados o si, por el contrario, carece de capacidad de adaptación para afrontar la creciente complejidad. El modelo vigente se ha diseñado para primar la protección de redes, sistemas y usuarios sobre cualquier otra dimensión, lo que justifica la mayoritaria presencia de actores públicos vinculados a la seguridad de la Figura 3 en el modelo. El resto de los actores como Exteriores, Industria, Educación, Ciencia, Economía, Justicia o Comercio forman parte del Consejo Nacional de Ciberseguridad, pero su influencia en la gobernanza es limitada. Si como parece, las políticas que se desarrollan en esos Ministerios influyen en la eficacia de la ciberseguridad, deberían contar con un mayor protagonismo e influencia en su gobernanza.

En modelos comparados como el del Global Cybersecurity Index, España figura entre los países que ofrecen un nivel superior de prestaciones legales, tecnológicas y organizativas, aunque con potencial crecimiento en el de las capacidades.[44] En relación con los objetivos previstos en la ENC vigente, el modelo ha preservado razonablemente bien la seguridad y la resiliencia del sector público y de los servicios esenciales (Objetivo I) así como la de sus activos críticos (Objetivo II), aunque también ha mostrado sus limitaciones durante la pandemia. Sin embargo, otros objetivos de la gobernanza como la protección del ecosistema empresarial y social (Objetivo III) o la regulación internacional del uso del ciberespacio (Objetivo V) no han tenido un progreso significativo.

La disparidad de los resultados obtenidos en los avances hacia los objetivos obedece a diversas causas. En primer lugar, la ENC vigente está más alineada con los objetivos regulatorios de la Estrategia Europea de 2020, los que tienen que ver con la trasposición o implantación de la abundante regulación europea, que con los objetivos con las dimensiones tecnológica, financiera, formativa, diplomática o de defensa de la misma Estrategia. En segundo lugar, el modelo cuenta con problemas estructurales como el ya mencionado desfase respecto a la digitalización, las diferencias de madurez entre

44 International Telecommunications Union, “Global Cybersecurity Index 2024”, pp. 24 y 124.

sectores y administraciones, la limitación de recursos y a la fragmentación de la gobernanza, con múltiples autoridades administrativas sin ninguna autoridad superior capaz de imponer la coordinación al resto[45].

A pesar de que España disponga de mayores capacidades de detección y respuesta que la mayoría de los países, los incidentes no paran de crecer tanto en el sector público como en el privado.[46] El crecimiento se explica porque la superficie de exposición crece más deprisa que las capacidades de protección, especialmente tras la aceleración de la digitalización por la pandemia, y porque las nuevas tecnologías facilitan los ciberataques.[47] La exposición a incidentes crece tanto en el sector público como en el privado de forma asimétrica: crece más en las administraciones locales y en las pymes que en la Administración General del Estado y las grandes empresas.[48]

El diferente grado de obligatoriedad en el cumplimiento modula las inversiones y la ampliación de los sujetos obligados y la superposición de entornos tecnológico de información (IT) y operativos (OT) aumentan el alcance del reto.

El Anteproyecto corrige algunas carencias de las anteriores, especialmente las que tienen que ver con la coordinación operativa, pero no afronta otras como las que se analizan a continuación.

4.1. El tsunami regulatorio

La dimensión regulatoria de la ciberseguridad presenta problemas de proliferación, armonización y supervisión que complican extraordinariamente su cumplimiento, especialmente por el sector privado. La regulación europea impulsa la nacional mediante la trasposición de directivas, la implantación de reglamentos o actos de implementación. A la proliferación normativa de la UE, creciente en cantidad y confusión, se deben añadir la nacional, cuando aprovecha su margen de autonomía para añadir nuevas capas de regulación

45 Como ejemplo de la atomización de autoridades de control en materia NIS, el RDL 12/2018 designaba 19 autoridades, muchas de las cuales no supervisarán a los operadores críticos. De hecho, la ESN de 2021 incluyo una línea de acción (la 17) para paliar la atomización y avanzar en la integración del modelo de gobernanza de la ciberseguridad en el marco del Sistema de Seguridad Nacional.

46 De los 177.098 incidentes registrados en 2024, el INCIBE-CERT gestionó 97.348 incidentes contra ciudadanos, empresas, redes académicas y operadores críticos y esenciales en 2024, un incremento del 16,6% respecto a 2023. En el sector público, el CCN-CERTgestionó 89.878 y el ESPDEF-CERT 983 según el Informe Anual de Seguridad Nacional 2024, pp. 113-119.

47 Según el Centro Criptológico Nacional, en 2024 se registró un incremento del 75% en los ciberataques respecto a 2023 debido a la integración de la inteligencia artificial. En contrapartida, la mejor calibración de las sondas de detección permitió reducir los falsos positivos en un porcentaje similar. Ciberamenazas y Tendencias, CCN-CERT IA-04-25, noviembre 2025, p. 5.

48 Más de 100.000 ciberataques en 2024 y uno muy grave cada tres días según el ministro de Transformación Digital, nota de prensa, (06/V/2025); un incremento del 16,6% en 2024 según el "Balance de Ciberseguridad de INCIBE" (26/III/2025).

y hay que temer la de las entidades subestatales que harán lo propio cuando puedan, lo que añadirá más complejidad y sobrerregulación.[49]

El proceso facilita la convergencia normativa con la UE, pero no la garantiza ni evita el solapamiento.[50] Las normas se acumulan y superponen en una dinámica que evoluciona más deprisa que la capacidad del Derecho digital europeo para responder o anticiparse.[51] Algunos sectores como el financiero se encuentran hiperregulados junto a otros como sanidad o trasporte prácticamente carentes de regulación o de normas técnicas ad-hoc.[52] En lugar de dar soluciones a la ciberseguridad, la sobrerregulación se ha convertido en un problema porque es ineficiente, genera inseguridad y pérdida de competitividad a quienes observan la diligencia debida en el cumplimiento normativo (compliance). Las empresas nacionales señalan el incumplimiento generalizado de de la regulación europea por compañías no establecidas en la UE y que ofrecen productos y servicios en Europa. Por lo tanto, urge revertir la tendencia, emprender una simplificación y armonización regulatoria basada en pocas normas que fijen mínimos de obligado cumplimiento de acuerdo con las directrices actualmente en debate en la propuesta de Directiva Ómnibus de la Comisión.[53]

La dimensión regulatoria no dispone de mecanismos para agilizar la armonización de las normas o asesorar sobre su cumplimiento, con lo que el sector privado, incluso las grandes organizaciones, se mueven en el filo de la inseguridad jurídica. A esto se añade la dificultad de la Administración para dialogar con el sector privado, tanto al inicio del trámite legislativo como durante su aplicación para supervisar el cumplimiento cuando sus recursos humanos no están a la altura de las exigencias de supervisión. La ordenación

49 Por ejemplo, en el Anteproyecto, España ha añadido añadir sectores no previstos expresamente en la Directiva NIS2 como la industria nuclear o la seguridad privada a la lista de entidades sujetas a obligaciones de gestión de riesgos y notificación de incidentes

50 El Esquema Nacional de Seguridad (ENS) ha demostrado su validez, pero supone un esfuerzo de certificación adicional para aquellas compañías que operan en múltiples geografías.

51 Andrés Moisés Barrio, "El cumplimiento basado en el riesgo o risk-based compliance, pieza cardinal del nuevo Derecho digital europeo", ARI 34, (20/IV/2023).

52 Por ejemplo, el sector del transporte de personas no cuenta con normas técnicas ad hoc, con lo que se reduce la competitividad de las empresas del sector. Las normas técnicas aseguran que los medios materiales de transporte ferroviario no dañen a las personas (safety); sin embargo, las normas no obligan por el momento a proteger estos equipamientos ferroviarios del daño derivado de los ciberataques ejecutados por personas (security), debido a criterios económicos (reducir gastos y CISOs) junto o a la dificultad y coste de certificar la ciberseguridad las infraestructuras OT al ritmo de las actualizaciones de sus sistemas de información.

53 La propuesta Ómnibus Digital persigue entre otros objetivos impulsar la simplificación de los informes de ciberseguridad derivados de la aplicación de la Directiva NIS2, el RGPD y DORA. La propuesta se concreta en tres puntos: (1) la unificación del canal de notificación de incidentes de ciberseguridad (se establece un punto de entrada único, las notificaciones de incidentes se trasladarían a las autoridades nacionales competentes a través de una plataforma única de entrada europea, establecida y mantenida por ENISA, que permitiría a las organizaciones cumplir simultáneamente con las obligaciones de reporte derivadas de la Directiva NIS2, el RGPD y DORA), (2) la mitigación del riesgo de incumplimiento por errores de procedimiento (la fragmentación normativa actual estaba generando complejidad en la gestión de plazos, destinatarios y contenidos de las notificaciones, aumentando la probabilidad de incumplimientos involuntarios que pueden derivar en sanciones administrativas), (3) nuevas exigencias para la planificación de recursos y formación interna (las organizaciones deberán adaptar sus procedimientos internos, protocolos de respuesta a incidentes y programas de formación para el personal responsable de las notificaciones).

en las distintas dimensiones que afectan a la ciberseguridad, entre ellas la gobernanza, la ciberseguridad de los productos, de las infraestructuras críticas, el acceso y uso de la IA o la retención de talento precisan un nuevo mecanismo normativo transversal, coordinado (evitar solapes) y convergente de las distintas regulaciones.

La implantación de las normas no suele acompañarse del seguimiento necesario para evaluar su rendimiento.[54] Los procesos regulatorios precisan un seguimiento público y privado que actualmente se lleva a cabo con dificultades tanto por la falta de personal especializado como por la diversidad de las materias reguladas y nuevos sectores obligados. A lo anterior se añade la exclusión de los destinatarios de la elaboración de las normas que les afectan hasta el momento de las consultas públicas, salvo relaciones bilaterales y personales no regladas. No es aceptable que mientras el sector privado dispone de un amplio nivel de interlocución regulatoria con la Comisión Europea en Bruselas desde el primer momento, tanto individualmente como a través de asociaciones sectoriales, ese sector privado tenga que esperar en España a que la Administración decida convocar consultas públicas para participar.

En el pasado, la presencia privada en las mesas sectoriales facilitaba la colaboración público-privada, pero el sector público ha ido excluyendo al privado de las iniciativas regulatorias. La desconexión entre reguladores y regulados impide conocer posiciones oficiales, alinear iniciativas y compartir valoraciones. La gobernanza regulatoria mejoraría si se articulan mecanismos de consulta entre ellos para intercambiar opiniones tanto antes de las obligadas consultas públicas, para evaluar su impacto, como después para facilitar su armonización y evaluar el seguimiento de sus resultados.[55] Si no se mejora la participación social, se corre el riesgo de que las grandes empresas y asociaciones trasladen su interlocución a Bruselas mientras que el resto del sector privado seguirá excluido hasta que el regulador quiera abrir el periodo de consulta pública.

Recomendaciones

La revisión de las estrategias de Seguridad Nacional y de Ciberseguridad debe garantizar la participación social en la elaboración y seguimiento de la regulación, al menos en las mismas condiciones de interacción inclusiva que ofrece la UE a los agentes privados.

54 Como ejemplo, la directiva NIS1 no contenía obligaciones de evaluar y publicar su impacto económico o cibernético a ninguno de los actores implicados y sólo se descubrieron sus carencias en la revisión de 2020.

55 El Foro Nacional de Ciberseguridad encargó a su grupo de trabajo sobre regulación que aportara valoraciones sobre la trasposición al grupo interministerial encargado de elaborarla. Nunca entraron en contacto directo, no se proporcionó información al sector privado y sus informes se difundieron al margen de la trasposición.

También debe establecer un mecanismo para facilitar la armonización de las distintas regulaciones y reducir la inseguridad jurídica derivada de los solapamientos.

4.2. Asimetría de costes y obligaciones

El modelo de gobernanza es cada vez más asimétrico en relación con el reparto de las obligaciones, los costes y las responsabilidades entre el sector público y el privado. La regulación endurece progresivamente las obligaciones, amplía sectores y entidades obligadas (esenciales e importantes), impone sanciones fuertes por incumplimiento (hasta el 2% de la facturación) y obliga a aplicar medidas técnicas y organizativas avanzadas, no solo básicas.[56]

El modelo ha desplazado la carga principal de la responsabilidad sobre las entidades medianas y grandes, sin que el sector público disponga de capacidad para apoyarlas, suplir las carencias de las administraciones de segundo nivel y supervisar el cumplimiento general de la regulación. El sector privado asume la mayor parte de las inversiones necesarias para proteger las infraestructuras y garantizar los servicios públicos sin que reciba ayuda significativa de quien tiene la responsabilidad y el monopolio de la seguridad nacional. En la práctica, el sector privado aporta más ciberseguridad de la que recibe, lo que encarece el cumplimiento de sus obligaciones.

Los incidentes no cesan de crecer, al igual que los costes de protección, sin que el Estado disponga de los medios necesarios para ejercer su obligación de proteger. En el nuevo contexto de confrontación geopolítica, los actores privados y las administraciones son objeto de ataques híbridos por su importancia para la seguridad nacional, no tanto por su condición privada. Los gobiernos no cuentan con los recursos necesarios para gestionar los riesgos de ciberseguridad al mismo tiempo que impulsan la digitalización y la economía digital. Hasta ahora, el modelo ha funcionado desplazando al sector privado los costes de la protección mediante la regulación, pero este enfoque asimétrico en las obligaciones y costes no puede seguir funcionando en el nuevo contexto de riesgos.

Mientras que en el sector privado se incrementa las responsabilidades y la rendición de cuentas de los responsables de ciberseguridad y las de altos

56 Niels Vandezande, “Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor”, Computer Law & Security Review, Volume 52, April 2024.

cargos, la legislación en vigor diluye la rendición de cuentas y la exigencia de responsabilidades del sector público, una tendencia que confirma el Anteproyecto. La asimetría preocupa especialmente que las administraciones de menor entidad y madurez puedan, cumplir sus obligaciones actuales y asumir otras nuevas como las de supervisión sin la debida exigencia. Sobre el déficit de rendición de cuentas públicas no se establecen indicadores de resultados, obligaciones de evaluación, ni responsabilidades políticas claras ante fallos sistémicos. Resulta difícil valorar los resultados del modelo objetivamente, positiva o negativamente, porque la política de ciberseguridad no dispone de una metodología de evaluación de sus objetivos, líneas de acción y medidas para reforzar las que sean eficaces, descartar las que no lo sean y añadir las que se precisen. En este sentido, los informes anuales elaborados por el Departamento de Seguridad Nacional proporcionan datos sobre lo realizado, pero no permiten medir el avance o retroceso sobre objetivos que se desconocen.[57]

La asimetría continúa en la profesionalización de los responsables públicos y privados. La ciberseguridad pública depende de órganos muy especializados como el CCN, CNPIC, OCC e INCIBE junto a otros órganos del sector público que a menudo carecen del personal y de la especialización necesaria. Es necesario profesionalizar las funciones de cargos de la Administración para dar continuidad en el tiempo a los planes y potenciar las capacidades más allá del calendario político. También ha de evitarse la superposición de funciones y competencias entre las administraciones porque el modelo de gobernanza no dispone de mecanismos de mediación para deslindarlas.58El modelo tampoco establece competencias a las autoridades sectoriales en materia de ciberseguridad OT, diferenciada ésta de la ciberseguridad IT, poniendo en riesgo la seguridad en sus dos acepciones (“safety” y “security”) y la resiliencia de numerosos sectores cuyas operaciones que descansan en infraestructuras OT, así como de los servicios esenciales que ofrecen sobre éstas.

Si la multiplicación creciente de riesgos, obligaciones y responsabilidades afecta a ambos sectores, ambos deben compartir también los costes y cargas asumidos proporcionalmente. El sector de la ciberseguridad privada se ha transformado, profesionalizado y financiado para atender las exigencias regulatorias, una adaptación que sólo han asumido algunos organismos del sector público.

57 La falta de trasparencia y de métricas podría evitarse si se aplicara la metodología de evaluación de la Ley 27/2022, de 20 de diciembre para la institucionalización de la evaluación de políticas públicas en la Administración General del Estado pero el modelo es renuente a su evaluación. Entre otras, la Estrategia de Ciberseguridad de Países Bajos utiliza la metodología oficial de evaluación de sus políticas públicas en la evaluación estratégica de su agenda. Netherlands Cybersecurity Strategy 2022-2028, p. 47.

58 Por ejemplo, el modelo de gobernanza de la Figura 3 está enfocada al mundo técnico ciber y mantiene su separación con el mundo de la resiliencia física (Reglamento CER).

Recomendación

El Estado, si no puede proteger a los actores privados frente a las amenazas del contexto geopolítico para la ciberseguridad, debe al menos compartir su coste, asumir sus responsabilidades y rendir cuentas en una proporción más equilibrada y menos asimétrica.

4.3. Gestión de incidentes

El modelo sigue gestionando los incidentes de forma insatisfactoria. Los procedimientos de notificación son demasiado complejos, con distintas autoridades, sin un procedimiento único y con limitada retroalimentación entre denunciantes e investigadores. La estructura de reportes de incidentes es acumulativa y muy compleja, con varias ventanillas cuando afecta a varias regulaciones (NIS, CER, GDPR, DORA, etc.).

En un contexto tan regulado y supervisado por el sector público, la responsabilidad de los incidentes no puede seguir atribuyéndose únicamente a las empresas afectadas por los incidentes. La responsabilidad de la diligencia debida es compartida y, en tiempos donde los ciberataques se dirigen por Estados y grupos paraestatales contra el Estado, debe aumentar su responsabilidad y liderazgo frente a estos grandes grupos responsables de los incidentes más graves. Si las medidas defensivas no bastan para disuadir los ciberataques, tendrá que ser el Estado el que aporte medidas ofensivas y el que apoye de verdad al sector privado cuando lo necesite.

El modelo de gobernanza es reactivo y orientado al cumplimiento normativo cuando se produce un incidente. La cooperación se fundamenta en la confianza recíproca, pero resulta difícil de compartir la respuesta a incidentes cuando la comunicación e información que se traslada al sector público puede ser usada en contra del denunciante a quien se puede ver como un infractor en potencia más que una víctima del ciberataque. El modelo no separa los roles de la(s) autoridad(es) regulatoria(s) del rol técnico y agregador (CERT) cuya función es ofrecer inteligencia y apoyo en la respuesta a los incidentes. La falta de separación entre la función técnica y la normativa permiten que quién apoya la gestión de incidentes sea juez a la vez.

Sin confianza, los responsables de la gestión tienen que dedicar más atención a las consecuencias sancionadoras de la supervisión que a la gestión del incidente. Las mismas autoridades que acompañan en la gestión pueden juzgar luego sobre la diligencia debida. Las autoridades han de ganarse la confianza de los afectados y para ello el único mecanismo práctico es separar los roles técnicos de los normativos, tal como evidencian los modelos de gobernanza adoptados en numerosos países de nuestro entorno según muestra la Tabla 1. Incluso en España, la experiencia de INCIBE muestra que la falta de competencias sancionadoras facilita la confianza en su gestión de incidentes con el sector privado.

Figura 4.

Ejemplos de países donde existe una separación entre el regulador de ciberseguridad y el regulador sectorial de la energía

PAÍSES	ÓRGANOS Y FUNCIONES
Reino Unido	**Órgano nacional: NCSC** (*National Cyber Security Centre*). Define el marco transversal de ciberseguridad, coordina respuesta a incidentes y emite guías técnicas. **Órgano sectorial: OFGEM** (*Office of Gas and Electricity Markets*). Pone en práctica las solicitudes en el sector energético, supervisa cumplimiento y aplica sanciones.
Alemania	**Órgano nacional: BSI** (*BundesamtfürSicherheit in derInformationstechnik*). Responsable de la estrategia nacional y respuesta a incidentes críticos. **Órgano sectorial: BNetzA** (*Bundesnetzagentur*, Agencia Federal de Redes de electricidad, gas, telecomunicaciones, ferrocarriles y correo postal). Supervisa la aplicación de la Ley de Seguridad de TIC en el sector energético, incluyendo requisitos específicos para operadores de red y generación.
Francia	**Órgano nacional: ANSSI** (*Agence Nationale de la Sécurité des Sytèmes d'Information*). Define el marco normativo general, emite estándares y guías, coordina la respuesta ante incidentes graves. **Órgano sectorial: CRE** (*Commission de Régulation de l'Energie*). Su papel principal es económico y técnico, pero en coordinación con ANSSI y bajo la *Loi de Programmation Militaire* (LPM) y la Directiva NIS2, supervisa que los operadores energéticos cumplan con las obligaciones de ciberseguridad.
Estados Unidos	**Órgano nacional: CISA** (*Cybersecurity and Infrastructure Security Agency*). Coordina la estrategia nacional y respuesta ante incidentes. **Órgano sectorial: NERC** (*North American Electric ReliabilityCorporation*). Aplica los estándares **NERC-CIP**, específicos para la industria eléctrica, bajo supervisión de FERC.

La preocupación del sector privado no tiene que ver con la resistencia a ofrecer transparencia sino a la mezcla de roles de las autoridades y el temor

a las sanciones. Hasta ahora, la falta de sanciones ha mitigado el riesgo, pero está situación podría cambiar en el futuro si el celo sancionador de la Administración exagera la exigencia de diligencia debida y quienes ayudan en los incidentes evalúan simultáneamente a los que asisten. El Anteproyecto aboga por reforzar la protección jurídica del notificante si actúa de buena fe, pero eso no suprime las dudas sobre la superposición de funciones. También establece una plataforma nacional de notificación y seguimiento de incidentes, lo que coadyuvará a facilitar la notificación.

Sin embargo, no está claro que la plataforma vaya a sustentar un sistema de inteligencia proactivo mediante el cual pueda el sector público alertar preventivamente sobre riesgos y amenazas al privado, tal y como aconseja la ENC vigente. Significativamente, el Anteproyecto no menciona la inteligencia en ningún apartado, aunque sí alude al intercambio de información, y es posible que la plataforma facilite al sector privado herramientas de inteligencia como Reyes del CCN-CERT que ahora se facilitan al sector público. En cualquier caso, algunos actores privados consideran que no hay suficiente cultura de inteligencia compartida, que su volumen es deficiente y que se limita a intercambios a través de los CSIRT y SOC, a lo que se añade la escasa voluntad de trasparencia pública y privada, lo que dificulta la compartición de inteligencia.

Recomendación

La gestión de los incidentes precisa un procedimiento que establezca derechos y obligaciones para los sectores público y privado, fomente los ejercicios y formación conjunta, comparta inteligencia proactiva, asegure el seguimiento y cuente con protocolos de comunicación estratégica para evitar alarmas sociales o empresariales innecesarias.

4.4. Sanciones y certificaciones

Las sanciones y las exigencias de certificaciones y estándares son otros puntos de la controversia público-privada. La dificultad de homogeneizar las sanciones en países europeos afecta a la competitividad de las empresas. En sentido contrario, la rigidez en la implementación afectaría a la competitividad de las empresas nacionales frente a países con trasposiciones más flexibles. El régimen sancionador no puede ser exclusivamente disuasorio porque necesita gradualidad (proporcionalidad) e incentivos positivos para su corrección que premien la diligencia debida. Lo mismo puede decirse respecto a la obligatoriedad de la formación de directivos en organizaciones que disponen de recursos limitados o al requisito de la

responsabilidad solidaria de los directivos en sectores regulados.[59] Sería preferible que el modelo tendiera a potenciar la colaboración público-privada que recompensara la proactividad de los agentes (modelos de autoevaluación y reportes voluntarios para recibir la ayuda de las agencias en caso de incidentes, auditorías expost, etc.).

También se debería clarificar qué estándares, certificaciones, tipos de auditorías, ratings y esquemas se pueden homologar, así como las buenas prácticas que garanticen un cumplimiento efectivo tanto en la gobernanza como en la gestión y en la operación.[60] La regulación debe acompañarse de plazos de adaptación realistas y de la asistencia técnica de los reguladores, lo que redunda en la necesidad de establecer canales de consulta público-privados. La adaptación debería prever el coste que supone la adaptación normativa para pymes en sectores críticos (el 15-20% sin incluir las cadenas de suministro) para alargar los procesos de transición y evitar sanciones por incumplimientos involuntarios (una flexibilidad similar, al menos, a la que se va a proporcionar necesariamente a las administraciones subestatales de menor tamaño y madurez).

Asimismo, es preciso evaluar la adecuación de las distintas certificaciones exigidas. Los actores nacionales – principalmente la Administración - se han acostumbrado a implantar el esquema nacional de certificación (ENS), pero éste resulta de difícil adopción para actores no españoles y las empresas nacionales establecidas en varios países prefieren un marco de certificación europeo o multinacional. El ENS necesitaría el reconocimiento europeo y/o un reconocimiento mutuo entre los distintos esquemas de certificación nacional. Igualmente importante sería homogeneizar los requisitos de las empresas sujetas a distintas certificaciones (PIC, NIS, DORA, GDPR y Directiva LED[61]) para evitar solapamientos. Se podrían estandarizar los requisitos convenientes para la certificación de sectores, para lo que sería aconsejable crear un grupo de trabajo sobre requerimientos y unas guías STIC para orientarlos. Las problemáticas de la certificación de tecnologías y procesos OT exigen una especial atención.[62]

---

59 La severidad de las infracciones a los directivos privados contrasta con la indulgencia frente a los públicos que no responden económica o solidariamente y sólo se exponen a posibles actuaciones disciplinarias en la redacción conocida del Anteproyecto.

60 El problema irá a más con la aprobación del Reglamento CRA cuyo ámbito son los productos y servicios. Se apuntan por potenciales soluciones a la certificación mediante la adopción de un esquema común europeo o esquemas nacionales simplificados (ej. LINCE del CCN). El inconveniente que tiene la segunda opción es que Francia y Alemania pueden descartar la certificación LINCE con lo que las pymes españolas se quedarán fuera.

61 Directiva (UE) 2016/680 de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo

62 En este sentido existe la oportunidad de tomar en el ámbito OT e IOT lo avanzado por PESI (Plataforma Española de Seguridad Industrial) el CCI (Centro Cyber Seguridad Industrial). Por ejemplo, en el sector del transporte ferroviario se ha creado un grupo de trabajo con más de 50 empresas fabricantes para ocuparse de los problemas del sector y los requisitos básicos. aunque cada una tiene su interés; identifican normas técnicas, regulación y afines, así como actores necesarios en el sector transporte (incluidos aquellos operadores sin responsables ciber) y finalmente a definir requisitos sectoriales.

Merece una mención específica la supervisión de riesgos de terceros en la cadena de suministro con el que las empresas han de demostrar la diligencia debida y que en la actualidad reside en las empresas contratantes. Ésta se articula mediante un mecanismo basado en extensos cuestionarios que han de completar las empresas que forman la cadena de suministro.
El número y detalle de los cuestionarios es creciente y muy costoso ya que los proveedores suelen desempeñar habitualmente el doble rol de suministrador y contratante. Sería de esperar que el Estado no se exonerara de este proceso y articulara un mecanismo de evaluación o certificación único por empresa.

En un modelo de gobernanza ampliada, se deberían reducir las cargas administrativas y económicas de la certificación, un aspecto muy gravoso para determinados sectores.[63] También se deberían armonizar los marcos regulatorios sectoriales, especialmente para operadores multirregulados (por ejemplo, banca o energía) para que no tengan que cumplir procedimientos diferentes para incidentes similares, estudiando la convalidación entre certificaciones para reducir costes y procedimientos.[64]

Recomendación

La actualización de la Estrategia de Ciberseguridad debe flexibilizar el régimen de sanciones, valorando los comportamientos proactivos, y simplificar el régimen de certificaciones para evitar costes y pérdidas de competitividad al sector privado.

4.5. La colaboración público-privada en retroceso

La colaboración público-privada retrocede respecto a los niveles de confianza e influencia anteriores. El distanciamiento entre Administración y administrados ha ido sustituyendo a colaboración directa y práctica de los primeros años entre los responsables públicos y privados de la protección de infraestructuras críticas, una socialización que se institucionalizó en el Foro Nacional de Ciberseguridad.La colaboración ha derivado hacia la apariencia,

63 Por ejemplo, la certificación ferroviaria obliga a aislar un tren durante meses y el proceso cuesta alrededor de dos millones de euros.

64 Aportaciones de la Confederación Española de Organizaciones Empresariales (CEOE) al Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad" (consulta pública NIS2).

y el distanciamiento. La cooperación vuelve a ser una concesión graciable -no un derecho reglado- del sector privado basado en realizar estudios desde el Foro, pero sin que la gobernanza lleve a caboun seguimiento de sus recomendaciones y que sigue sin tener influencia en el proceso de decisiones.

El Anteproyecto añade el CNC a los organismos ya existentes que carecen de una representación reglada del sector privado, lo que parece contrastar con la masiva aportación de inversiones del sector privado y el impacto de la regulación sobre este sector. La fragmentación -o las rivalidades-del sector público afectan a su relación con el sector privado porque las entidades que ofrecen servicios esenciales son muy numerosas, y algunas de ellas tienen que reportar a más de una de las numerosas entidades de control sectoriales.

La cooperación público-privada no es un adorno procedimental, sino un mecanismo democrático de gobernanza. La mayor parte de las infraestructuras, de los datos y de las capacidades técnicas relevantes para la ciberseguridad se encuentran en manos de empresas y operadores privados. Sin su participación estable en el diseño, la implementación y la evaluación de las políticas, el sistema queda condenado a una brecha permanente entre lo que las normas exigen y lo que es viable en la práctica. La cooperación entre el sector público y el sector privado debe ir más allá de las consultas informales y de la participación simbólica en foros amplios. Se trata de construir espacios de codecisión y corresponsabilidad en los que el sector privado participe en la definición de riesgos prioritarios, en el diseño de medidas proporcionadas, en la detección de efectos no deseados de la regulación y en la movilización de recursos para la prevención y la respuesta. Todo ello con las medidas de confidencialidad y discreción que exige un ambiente de confianza[65].

No se trata de acceder a la corregulación, pero sí a que los agentes regulados sean escuchados por los reguladores a lo largo del proceso oficial de decisiones, especialmente desde el principio para que valoren el impacto de las medidas sobre sus destinatarios. No se trata de compartir la supervisión, sino de contar con mecanismos transparentes de evaluación y diferenciar las funciones de supervisión de las operativas. Supone clarificar el papel y las funciones de los órganos de cooperación existentes, dotarlos de capacidad real de influencia sobre el ciclo de las políticas e integrarlos de forma orgánica en la arquitectura de dirección política[66]. Solo así la ciberseguridad dejará de tener una agenda definida casi exclusivamente por los actores públicos y pasará a ser una responsabilidad compartida con quienes gestionan, desarrollan y explotan las infraestructuras y servicios digitales privados sobre los que descansa la seguridad del país.

65 El Foro funciona con acuerdos de confidencialidad diseñados para una mayor influencia en el proceso de decisiones que parecen excesivos para la elaboración de estudios y recomendaciones.

66 La Estrategia de Ciberseguridad Francesa 2026-2030 incorpora al sector privado (grandes operadores, academia, sociedad civil) en el grupo de actores esenciales para el desarrollo e implementación de la respuesta contra las ciberamenazas (Multi-staque governance in the service of national resilience, p..29)

Recomendación

> Las estrategias de Seguridad Nacional y de Ciberseguridad deben garantizar la participación reglada del sector privado en la elaboración de estrategias, políticas, normas y agendas que le afecten, a tiempo de influir en su diseño y con un procedimiento que garantice la confidencialidad debida.

4.6 Las asignaturas pendientes

La gobernanza no ha sabido hasta ahora resolver el problema de la ciberseguridad de las cadenas de suministro, una de las principales vías de entrada de ciberataques en la actualidad, que expone a la totalidad del tejido industrial. No resulta fácil exigir garantías de ciberseguridad a todas las pymes ni pedir a las entidades tractoras que exijan su cumplimiento. Las empresas consultadas indican que la actual regulación (NIS2, CER) pone excesivo foco en las entidades críticas y esenciales que sufren los ataques, siendo necesario adoptar una aproximación que asuma responsabilidades distribuidas y que proteja a la totalidad del tejido industrial, en particular pymes y empresas exentas del ámbito de NIS2. Mientras que el Esquema Nacional de Seguridad exige garantías a todas las empresas, el marco regulatorio tras la NIS2 excluye a las pymes de menos de 50 empleados, lo que preserva la inseguridad de las cadenas de suministro y pone a esas empresas en riego de exclusión de las cadenas de suministro de empresas reguladas.

Tampoco ha sabido dar respuesta al problema estructural de la ciberseguridad industrial (OT), cuyos elementos profusamente desplegados en las empresas y en particular en operadores de infraestructuras críticas son particularmente vulnerables a los ciberataques. Esta situación es especialmente grave si se tiene en cuenta que la mayor parte de elementos OT carecen de posibilidades de instalar actualizaciones que eviten la explotación de vulnerabilidades, previsiblemente crecientes en número e impacto por el uso de IA agentica. La coordinación y gestión de incidentes OT es una fuente adicional de preocupación ya que no se adapta al actual modelo de gestión establecido principalmente para incidentes del ámbito IT. Se precisan herramientas y procedimientos que den una respuesta global adecuada a incidentes en ámbitos conjuntos IT, OT y en la cadena de suministro.A los retos que ofrecía la aplicación de la inteligencia artificial (IA) a la ciberseguridad se ha unido su aplicación reciente al ámbito ofensivo, lo que proporciona a las amenazas estatales y criminales

capacidad para acelerar, escalar y automatizar sus operaciones ofensivas.67 La automatización plantea un cambio de paradigma a los responsables públicos y privados de la ciberseguridad. La proliferación de modelos de IA agentica, la inminente aplicación de la computación cuántica, el incremento de las vulnerabilidades descubiertas o la reducción de los tiempos de respuesta obligan a revisar los modelos de gobernanza. El desafío supone un cambio cultural, el recurso a la IA defensiva y la convicción de que todos los sistemas se van a ver comprometidos, por lo que el enfoque tiene que ser de resiliencia. Paralelamente, el uso ofensivo de la IA aumenta el riesgo para la autonomía estratégica nacional de la dependencia tecnológica e industrial de terceros.

Recomendación

Las estrategias de Seguridad Nacional y de Ciberseguridad deben adoptar medidas para afrontar los desafíos estructurales que presentan las cadenas de suministro y la ciberseguridad industrial OT, así cómo integrar tecnologías disruptivas como la inteligencia artificial o la computación cuántica en la gobernanza de la ciberseguridad

67 CCN-CERT, “Guía de buenas prácticas frente al modelo de IA ofensiva”, Guía de seguridad BP/36, junio 2026.

Conclusiones y recomendaciones

El gobierno y las autoridades responsables de la ciberseguridad deberían aprovechar el momento actual - aprobación del Anteproyecto para la nueva Ley de coordinación y gobernanza de la ciberseguridad, actualización de la Estrategia Nacional de Ciberseguridad, y desarrollo reglamentario del Centro Nacional de Ciberseguridad - para adoptar las recomendaciones apuntadas en el documento, que se formulan desde una perspectiva privada para ampliar las dimensiones del modelo de gobernanza y mejorar su funcionamiento.

Recomendaciones para ampliar las dimensiones y atenuar las asimetrías del modelo de gobernanza:

1. Las futuras estrategias de Seguridad Nacional y Ciberseguridad Nacional deberían corregir las carencias del modelo de gobernanza vigente para superar sus contradicciones y afrontar los desafíos que plantean las nuevas dimensiones de la ciberseguridad.

2. La ciberseguridad debería contar con una partida presupuestaria que consolidara anualmente un nivel de inversión entre 1.000-1.500 millones de euros para aportar al sector la estabilidad financiera que precisa.

3. El Gobierno debe adoptar un PERTE que permita integrar la base industrial y tecnológica de la ciberseguridad y la ciberdefensa en una política industrial a largo plazo que fomente la autonomía estratégica mediante la colaboración público-privada.

4. La Estrategia de Seguridad Nacional debe definir el concepto de ciberdefensa activa, diferenciar el ámbito civil del militar y regular el uso de los instrumentos ofensivos y defensivos.

5. Las capacidades de ciberdefensa precisan una base industrial y tecnológica (hub) que asegure el máximo nivel de autonomía estratégica posible en la defensa nacional y que, a su vez, retroalimente las capacidades civiles de ciberseguridad.

6. La estructura del Ministerio de Asuntos Exteriores debe adecuar sus recursos al protagonismo que la ciberdiplomacia debe asumir en la gestión internacional y doméstica de las políticas para la ciberseguridad.

7. La Estrategia de Ciberseguridad debería reivindicar un papel más activo a la Administración de Justicia para apoyar a la Fiscalía y cuerpos policiales en su lucha contra la cibercriminalidad, para evitar que el desfase entre las conductas criminales y la respuesta procesal y penal se agrave con los cambios tecnológicos en curso y ponga en riesgo las investigaciones criminales y la confianza social en la digitalización.

8. Las estrategias de Seguridad Nacional y de Ciberseguridad deben garantizar la participación social en la elaboración y seguimiento de la regulación, al menos con los mismos niveles de interacción inclusiva que ofrece la UE a los agentes privados. También deben articular un mecanismo de armonización y simplificación del marco normativo.

9. El Estado, si no puede proteger a los actores privados frente a las amenazas del contexto geopolítico para la ciberseguridad, debe al menos compartir su coste, asumir sus responsabilidades y rendir cuentas en una proporción más equilibrada y menos asimétrica que la actual.

10. La gestión de los incidentes precisa un procedimiento que establezca derechos y obligaciones para los sectores público y privado, fomente los ejercicios y formación conjunta, comparta inteligencia proactiva, asegure el seguimiento y cuente con protocolos de comunicación estratégica para evitar alarmas sociales o empresariales innecesarias.

11. El modelo regulatorio debe flexibilizar el régimen de sanciones, incentivando los comportamientos proactivos, y simplificar el régimen de certificaciones para evitar costes y pérdidas de competitividad al sector privado.

12. Las estrategias de Seguridad Nacional y de Ciberseguridad deben asegurar la participación reglada del sector privado en la elaboración de estrategias, políticas, normas y agendas que le afecten, a tiempo de influir en el diseño y con un procedimiento que garantice la confidencialidad debida.

13. Las mismas estrategias deben adoptar medidas para afrontar los desafíos estructurales que presentan las cadenas de suministro y la ciberseguridad industrial OT, así como integrar tecnologías disruptivas como la inteligencia artificial o la computación cuántica en la gobernanza de la ciberseguridad.

Autores

Félix Arteaga, investigador, Real Instituto Elcano.
Javier Alonso, investigador sénior no residente, Real Instituto Elcano.

Cita recomendada:
Arteaga, F. y J. Alonso (2026), "Por una gobernanza ampliada de la ciberseguridad", *Elcano Policy Paper*, Real Instituto Elcano

Patronato

GOBIERNO DE ESPAÑA — MINISTERIO DE ASUNTOS EXTERIORES, UNIÓN EUROPEA Y COOPERACIÓN

GOBIERNO DE ESPAÑA — MINISTERIO DE DEFENSA

GOBIERNO DE ESPAÑA — MINISTERIO DE CULTURA

GOBIERNO DE ESPAÑA — MINISTERIO DE ECONOMÍA, COMERCIO Y EMPRESA

ACERINOX · ACS · AIRBUS · amazon

BBVA · BANCO DE ESPAÑA Eurosistema · CaixaBank · Cámara de Comercio de España

em&e group · enagas · endesa · GARRIGUES

Hijos de Rivera · Iberdrola · IBM · INDITEX

INDRA GROUP (INDRA | MINSAIT) · INSUD PHARMA · MADRID · moeve

MUTUAMADRILEÑA · Naturgy · oesia grupo · PROSEGUR

renfe · repsol · Santander · Telefónica

Socios protectores

acciona · CAF Banco de Desarrollo de América Latina y el Caribe · El Corte Inglés · Sabadell

Socios colaboradores

ABANCA · aena · ceca · cesce Seguros de tu éxito · Deloitte. · Fundación Ibercaja · Google · KPMG · mapfre · NETFLIX · ULMA

Real Instituto Elcano
C/ Príncipe de Vergara, 51
28006 Madrid
www.realinstitutoelcano.org

REAL INSTITUTO
elcano
ROYAL INSTITUTE

25
AÑOS·YEARS