Documento de trabajo 4/2019
11 de febrero de 2019

Propuestas desde el sector privado para la revisión de la Estrategia de Ciberseguridad Nacional

Félix Arteaga y Javier Alonso Lecuit (coords.)

Propuestas desde el sector privado para la revisión de la Estrategia de Ciberseguridad Nacional

Félix Arteaga y Javier Alonso Lecuit han coordinado la elaboración de este Documento, en el que han participado los miembros del Grupo de Trabajo de Ciberpolítica del Real Instituto Elcano que representan al sector privado.

Índice

Resumen

La revisión de la Estrategia de Ciberseguridad Nacional de 2013 es una buena oportunidad para incluir en su elaboración a la mayor parte posible de implicados. Sólo una amplia participación del sector público y privado (*whole-of-nation approach*) daría a la Estrategia un carácter inclusivo y "nacional" (Estrategia *Nacional* de Ciberseguridad), mientras que una participación restringida a la Administración (*whole-of-government approach*) prorrogaría el enfoque gubernamental de la Estrategia de Ciberseguridad Nacional en 2019.

Introducción

La ECN de 2013 vino a resolver los retos de ciberseguridad asociados con la protección de las infraestructuras críticas y los servicios esenciales para la población vinculados a la seguridad nacional. Era la primera estrategia y tenía como prioridad articular los elementos esenciales del sistema de ciberseguridad nacional y los primeros planes y medidas del sector. Pasados seis años, la ECN debe responder también al actual contexto de la ciberseguridad, adaptarse a la mayor complejidad y diversidad de aspectos que gestionar y aprovechar las lecciones aprendidas de la experiencia durante estos años.

El sector privado no participó en la elaboración de la ECN de 2013, probablemente debido a la urgencia y el enfoque de seguridad nacional predominante. Desde entonces, se ha incrementado el número de actores privados implicados por la expansión de la ciberseguridad desde la seguridad nacional a la seguridad económica. La trasposición de la Directiva NIS, en la que tampoco participó el sector privado, puso de relieve la necesidad de que este sector adoptara una posición más asertiva, porque ahora las decisiones del sector público afectan también a la competitividad, la cuenta de resultados y los modelos de negocio de las empresas en general y de las industrias de ciberseguridad, en particular las cadenas de suministro y los proveedores de servicios esenciales y digitales, así como los centros tecnológicos y de investigación.

El presente Documento de Trabajo recoge una primera aproximación a la posición del sector privado elaborada en el marco del Grupo de Trabajo de Ciberpolítica del Real Instituto Elcano que precisaría una mayor contrastación. El sector privado tampoco ha participado como grupo organizado en la revisión de la ECN en curso, salvo un grupo de expertos individuales que no representan necesariamente la posición del sector en su conjunto. En el Documento se recogen y explican las valoraciones del sector sobre el estado actual de la ciberseguridad y las propuestas de adaptación y mejora que debería recoger la futura ECN para fomentar su apropiación por el sector privado.

Sumario ejecutivo

Las propuestas del sector privado para la Estrategia de Ciberseguridad Nacional (ECN) de 2019 tienen como finalidad modificar los objetivos, principios y líneas de acción de la ECN de 2013 (en la columna de la izquierda) y añadir nuevas propuestas, que se recogen en las tablas siguientes (columna de la derecha).

Tabla 1. Objetivos de las estrategias

Objetivos	**ECN 2013**	**ECN 2019**
I y II	Garantizar que los sistemas de información y telecomunicaciones que utilizan las Administraciones Públicas poseen el adecuado nivel de ciberseguridad y resiliencia	El objetivo de la ECN debe ampliarse de garantizar la seguridad y resiliencia de la información y los sistemas (IT) utilizados por el sector público y privado a la seguridad industrial (OT) y la seguridad digital de objetos conectados (IoT e IIoT) **(la ciberseguridad es trasversal)**
III	Impulsar la seguridad y resiliencia de los sistemas de información y telecomunicaciones usados por el sector empresarial en general y los operadores de infraestructuras críticas en particular	
IV	Potenciar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente a las actividades del terrorismo y la delincuencia en el ciberespacio	El objetivo de la ECN debe ampliarse de la protección de las infraestructuras críticas frente al terrorismo y la delincuencia (seguridad nacional) a proteger los intereses y oportunidades económicas para la industria, servicios y tecnología (seguridad económica) **(las infraestructuras críticas son una parte de la ciberseguridad y no al revés)**
V	Sensibilizar a los ciudadanos, profesionales, empresas y Administraciones Públicas españoles de los riesgos derivados del ciberespacio	La ECN debe pasar de sensibilizar frente a los riesgos derivados del ciberespacio a exigir responsabilidades a las Administraciones, empresas e industrias que participan en las cadenas de suministro de ciberseguridad **(de la concienciación al compromiso)**
VI	Alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita España para sustentar todos los objetivos de ciberseguridad	La ECN debe identificar, proteger e impulsar mediante la I+D+i el desarrollo de aquellas tecnologías críticas para la ciberseguridad nacional que no deban depender de terceros y fomentar la cooperación internacional del sector industrial con socios estratégicos **(soberanía tecnológica)**

Tabla 2. Principios rectores de la ECN

	ECN 2013	ECN 2019
Liderazgo y coordinación de esfuerzos	El ámbito y la complejidad de los desafíos del ciberespacio requieren un liderazgo nacional decidido y la adecuada coordinación de las capacidades, recursos y competencias involucrados. Ambas exigencias son asumidas por el presidente del Gobierno, que dirigirá y supervisará la Política de Ciberseguridad Nacional en el marco del Consejo de Seguridad Nacional	El Sistema de Ciberseguridad Nacional está superado por el desarrollo y la complejidad de la ciberseguridad y debe centralizarse para superar las dificultades de coordinación interministerial (centralización del Sistema de Ciberseguridad Nacional) La centralización facilitaría la gobernanza en los aspectos de seguridad nacional, pero la gobernanza general de todos los aspectos de la ciberseguridad, incluidos los que tienen que ver con la seguridad económica y con la participación de los actores no gubernamentales del ecosistema, precisa la creación de una agencia público-privada (creación de una Agencia de Ciberseguridad)
Responsabilidad compartida	Todos los agentes públicos y privados con responsabilidad en esta materia, incluyendo también a los propios ciudadanos, han de sentirse implicados con la ciberseguridad. Para ello, se hace precisa una intensa coordinación de los diferentes organismos de las Administraciones Públicas y una adecuada cooperación público-privada capaz de compatibilizar iniciativas y propiciar el intercambio de información	La ECN debe regular la participación del sector privado en los niveles y procesos de decisión que los afecten, especialmente de las empresas que son sujetos principales de las obligaciones regulatorias, con un enfoque más proactivo e inclusivo, particularmente en las funciones de gestión estratégica, gestión de crisis y regulación que afecte a su seguridad económica (la participación privada es obligatoria según la Ley de Seguridad Nacional y debe regularse)

	ECN 2013	ECN 2019
Proporcionalidad, racionalidad y eficacia	Es necesario gestionar los riesgos derivados del uso de la tecnología de forma dinámica, equilibrando oportunidades y amenazas y asegurando la proporcionalidad en las medidas de protección adoptadas, que habrán de ser elementos habilitantes de la confianza y no trabas al desarrollo de nuevos servicios	Para equilibrar amenazas y oportunidades, la ECN debe evitar que la cultura predominante de seguridad física invada espacios que no son de amenazas (seguridad nacional), sino de oportunidades (seguridad económica). Para hacerlo, debe regular la obligación de contar con perfiles profesionales adecuados a la evolución de la ciberseguridad (definición y capacitación de los responsables públicos y privados) La proporcionalidad en las medidas de protección frente a un incremento constante de los ciberataques obliga al sector público a elevar su nivel de disuasión regulando la defensa activa (*hack-back*) y consolidando instrumentos de ciberdiplomacia y ciberdefensa en situaciones de particular gravedad. Del mismo modo, corresponde al sector público establecer las certificaciones de carácter crítico relacionadas con la ciberseguridad de las cadenas de suministro (la participación privada complementa, pero no reemplaza, a la pública en las funciones de seguridad nacional)
Cooperación internacional	El carácter transfronterizo de las amenazas hace que sea esencial promover la cooperación global, ya que muchas de las posibles medidas sólo resultarán eficaces si se adoptan internacionalmente con la adecuada cooperación y coordinación entre los distintos países	La ECN debe pasar de fomentar la cooperación transfronteriza por razón de las amenazas a su fomento por razón de las oportunidades económicas que ofrece para potenciar su base tecnológica e industrial (dotar a la cooperación internacional de una dimensión de inteligencia económica)

Tabla 3. Líneas de acción de la ECN

	ECN 2013	ECN 2019
1	Capacidad de prevención, detección, respuesta y recuperación ante las ciberamenazas	Ampliar el ámbito de esas capacidades, así como las de inteligencia, a sistemas de defensa activa o certificaciones críticas, al sector privado de interés estratégico **(llegar donde la capacidad privada no llega)**
II-III	Seguridad de los sistemas de información y telecomunicaciones que soportan las Administraciones Públicas y las infraestructuras críticas	Verificar el cumplimiento de las medidas de seguridad acordadas para proteger los sistemas públicos y privados con el fin de asegurar que ambos sistemas cumplen sus compromisos **(mecanismo de evaluación)**
IV	Capacidad de investigación y persecución del ciberterrorismo y la ciberdelincuencia	Potenciar la colaboración del sector privado en esas capacidades restringiendo el ámbito, compensando los costes y no pidiendo más colaboración de la que se pueda aprovechar. En sentido inverso, el sector público debería facilitar al privado la inteligencia que precisa en la gestión de crisis y en la tramitación de denuncias **(la colaboración debe ser de doble sentido)**
V	Seguridad y resiliencia de las TIC del sector privado	Centralizar, consensuar y simplificar la colaboración público-privada (**ventanilla única, procedimientos pactados, denuncias y retroalimentación**) Implantar una infraestructura de certificación concertada con el sector privado
VI	Conocimientos, competencias e I+D+i	Dedicar parte del presupuesto de ciberseguridad nacional a preservar la base tecnológica e industrial de la ciberseguridad **(sin presupuestos ni estrategias de inversión no hay políticas de I+D+i)** Completar e integrar el ecosistema de ciberseguridad y las iniciativas de colaboración en curso (Red de Excelencia Nacional de Investigación en Ciberseguridad, RENIC; Asociación Empresarial Innovadora en Ciberseguridad y Tecnologías Avanzadas, AEI Ciberseguridad; equipos de respuesta e incidentes de seguridad, red CSIRT.es) para posicionar el ecosistema nacional en el nuevo contexto europeo y global Establecer acuerdos y alianzas estratégicas con los suministradores internacionales de referencia y confianza que permitan desarrollar el tejido empresarial nacional y facilitar su acceso a la tecnología y mercados **(partenariados)**

Tabla 4. Líneas de acción adicionales para la ECN 2019

1	Reforzar las medidas exigibles a las empresas del sector privado que sean de interés, estratégicas o críticas para la cadena de suministro de la industria y servicios de la ciberseguridad	Obligación legal de presentar un informe o plan de ciberseguridad periódico (anual) a los consejos de administración de las sociedades que cotizan y a la presidencia de las agencias públicas **(la ciberseguridad es un activo estratégico)** Obligación legal de todas las empresas, y en particular aquellas que participan en las cadenas de suministro de ciberseguridad, de tener un CISO, una organización, un plan de riesgos y un compromiso de supervisión y actuación de su directiva **(todos rinden cuentas y más cuanta más relevancia tienen para la ciberseguridad)**
2	Evitar la hiperregulación unilateral del sector público	La regulación del sector privado debe establecer el marco general de control (organización, condiciones, responsabilidades, buen gobierno…), pero dejar su cumplimiento al criterio de las empresas **(la norma fija el qué y las empresas, el cómo)** Para ello es necesaria la implicación del sector privado desde los primeros momentos en el proceso regulatorio que lo afecte **(tanto en España como en la UE)**
3	Dotación presupuestaria independiente, como cualquier otra política pública	La ECN deberá acompañarse de una memoria económica con los distintos objetivos de gasto y su distribución **(sin presupuesto no hay política)** Los objetivos y líneas de acción de la ECN deben objetivarse (medidas, responsables y recursos asignados) y contar con un sistema de evaluación para medir su progresión **(sin supervisión tampoco)**

Criterios para la revisión de la ECN de 2013 desde el sector privado

Al igual que el sector privado europeo, al menos el representado por la European Cyber Security Organization (ECSO), viene exigiendo su participación en la elaboración de una estrategia europea de ciberseguridad[1], el sector privado nacional considera que debe contribuir a la revisión de la ECN de 2013. Su revisión se justifica por la evolución del contexto de ciberseguridad **(criterios de adaptación)** y por la evaluación de las lecciones aprendidas desde 2013 **(criterios de mejora)**.

Entre los primeros, la futura ECN debe ampliar su objeto de la información y los sistemas (IT) a la seguridad industrial (OT) y la seguridad digital (IIoT e IoT), incluyendo la ciberseguridad de los productos fabricados por la industria nacional[2]. La ampliación del espectro de riesgos obliga a reforzar el enfoque preventivo implantando la ciberseguridad por diseño como requisito obligatorio de la compra pública de bienes, instalaciones e infraestructuras[3] y en todas las empresas que participan en las cadenas de suministro asociadas a la ciberseguridad[4].

La adaptación al nuevo contexto obliga a equilibrar el enfoque/cultura de infraestructuras críticas predominante hasta ahora en el conjunto de la ciberseguridad para evitar que invada espacios que no son de seguridad nacional, sino de seguridad económica[5]. En el mismo sentido, el incremento y la aceleración de los cambios mencionados, unidos a los regulatorios y a la proliferación de relaciones institucionales, desborda la capacidad de gestión del modelo actual de coordinación. En consecuencia, **se necesita centralizar el Sistema de Ciberseguridad Nacional** en los aspectos que tienen que ver con el núcleo de la seguridad nacional y el sector público, de forma que se refuercen las competencias de coordinación de las autoridades coordinadoras. Lo anterior reduciría las fricciones dentro del sector público y facilitaría la gestión interministerial. Por otro lado, y para potenciar el resto del ecosistema nacional de ciberseguridad, **se necesita crear una Agencia de Ciberseguridad**.

[1] European Cyber Security Organization, "ECSO convened its first High Level Roundtable on Europe's Cyber Future", 7 de febrero.

[2] El reto de la ECN es afrontar la ampliación del espectro de riesgos hacia la seguridad industrial u operacional (OT), porque los riesgos de algunas instalaciones industriales, en edificios o espacios públicos, tienen tanto o más impacto sobre la seguridad pública que los de las infraestructuras críticas.

[3] Hasta ahora, se recomienda —pero no se obliga a— incluir los requisitos de ciberseguridad en los contratos del Esquema Nacional de Seguridad (RD 3/2010 y CCN-STIC 830) y en algunos contratos (normalmente, los *grandes*), pero no en otros, debido a la fragmentación de la contratación/subcontratación, lo que crea brechas de seguridad sobrevenidas. En el mismo sentido, la ciberseguridad no debe contratarse en un acto posterior —añadiendo *capas*— ni esperar a que haya disponibilidad presupuestaria para hacerlo.

[4] La regulación, obligatoria, es necesaria debido a criterios de seguridad (las empresas menos concienciadas son el eslabón más débil), de competitividad (las empresas menos fiables restan reputación al producto final) y de obsolescencia (debido al acortamiento exponencial de la vida de las empresas y productos). La obligatoriedad ya se ha implantado con éxito en el caso de la LO de Protección de Datos, lo que demuestra la viabilidad de este modelo normativo.

[5] La cultura de infraestructuras críticas (seguridad física) ha predominado en la ECN de 2013 —la Ley PIC es de 2011— y está aprovechando el RDL 12/2018 para ampliar su ámbito de actuación al margen de lo dispuesto en la Directiva NIS. Sus miembros aspiran a ocupar los puestos de responsables de seguridad de la información (art. 16.3 del RDL 12/2018) y los relacionados con la ciberseguridad OT e IoT.

(cont.)

La valoración de la ECN de 2013 es generalmente positiva, pero se podría mejorar en los aspectos siguientes. Primero: la ECN no ha contado con un sistema de evaluación y supervisión que permitiera medir sus avances y mejorar su eficacia. La valoración de las estrategias, del Plan de Ciberseguridad Nacional o de los planes sectoriales no depende tanto de las medidas adoptadas en ellos (rodeado de secretismo y escasa trasparencia), sino de su cumplimiento, por lo que será necesario respaldar la gestión con un **mecanismo de evaluación**. Ese mecanismo permitiría establecer un sistema de métricas y una cronología para valorar el progreso hacia los objetivos y líneas de acción definidos en la ECN. Segundo: la cooperación público-privada sigue sin contar con la regulación prevista en la Ley de Seguridad Nacional (art. 7), con lo que el sector privado no participa en las decisiones que lo afectan y la regulación se le presenta como un hecho consumado **(la gestión no es inclusiva)**[6]. Tercero: el desarrollo de las líneas de actuación de la ECN de 2013 no ha atendido debidamente los riesgos derivados de la dependencia tecnológica ni de la disrupción tecnológica[7]. Como propone ECSO, la ciberseguridad es un sector industrial que precisa impulsarse con una política industrial para aumentar la competitividad y otra de compra pública para fomentar una "IT made in Europe". En consecuencia, la ECN de 2019 deberá potenciar una base tecnológica e industrial nacional de ciberseguridad mediante programas específicos de investigación, desarrollo e innovación (I+D+i) y de adquisiciones, así como fomentar acuerdos internacionales que faciliten a la industria nacional el acceso a tecnología y mercados[8] **(soberanía tecnológica e industrial)**.

Modelo de gobernanza

El modelo ha sido objeto de una elaboración y discusión previa dentro del Grupo de Trabajo, por lo que ahora sólo se mencionan aquellas sugerencias que tienen que ver con su tratamiento en la ECN.

La coordinación interministerial ha mejorado su funcionamiento, pero el sector privado sigue percibiendo que las divergencias e intereses particulares afectan al desarrollo de la ciberseguridad, duplican las estructuras (demasiados CERT cuando se podría funcionar con uno) y consumen recursos escasos en la Administración. La coordinación interna podría mejorar si se dota al presidente del Consejo de Ciberseguridad Nacional de un comité permanente de asesoramiento que facilite la conducción, supervisión y evaluación de la política de ciberseguridad, el enfoque estratégico y las lecciones aprendidas, **un comité en el que es indispensable la participación privada**[9].

[6] La regulación se exige por el art. 7.1 de la Ley de Seguridad Nacional ("El Gobierno establecerá reglamentariamente los mecanismos y formas de esta colaboración").

[7] Por ejemplo, la aplicación al ámbito de la ciberseguridad de tecnologías habilitadoras tales como la inteligencia artificial, *big data*, esquemas de cifrado cuántico o computación cuántica para el descifrado.

[8] Se deben potenciar soluciones nacionales para nichos críticos de seguridad y de negocios para hacer converger las inversiones públicas y privadas (invertir en los *agujeros* de ciberseguridad y en los nichos tecnológicos que el mercado no cubre). La ciberseguridad debe integrarse en los planes nacionales de investigación, los programas duales del CDTI y el Horizonte Europa de la UE.

[9] El comité o agencia facilitaría la función permanente de coordinación y permitiría abordar la de supervisión (evaluación de objetivos, planes, medidas y progreso del Plan de Ciberseguridad Nacional), que sigue pendiente.

En segundo lugar, se observa una seria preocupación en el sector privado por la gestión de cibercrisis graves. No existe un protocolo de actuación que se extienda más allá de la gestión del propio ciberincidente, es decir, en el que los órganos de gobierno o grupos *ad hoc* realicen un seguimiento y evaluación, formal e informal, de dichas crisis. En situaciones de crisis, el sector privado percibe que las decisiones están vinculadas a la proactividad y toma de decisión de personas individuales mediante mecanismos informales, no al seguimiento de unos protocolos establecidos, con lo que se corre el riesgo de que el sistema pueda llegar a paralizarse. Se observan diferencias de opiniones sobre la gestión —positiva o negativa— del incidente WannaCry. La coincidencia es mayor en la necesidad de haber aprendido la lección y establecido sistemas fiables y resilientes de comunicaciones, así como en la utilidad de los ciberejercicios, pero **se echa de menos una mayor reflexión conjunta en torno a la gestión de crisis con la Administración**[10].

Debido a la expansión de la ciberseguridad hacia sectores que no tienen que ver con la seguridad nacional, el Sistema de Ciberseguridad Nacional —incluso centralizado— no debería gobernar en solitario aspectos que afectan fundamentalmente a las empresas, industrias, centros tecnológicos e I+D+i, entre otros, del sector privado, por lo que habría que avanzar hacia un **modelo de Agencia de Ciberseguridad**[11]. Sólo una agencia puede abarcar la complejidad e importancia que está alcanzando la ciberseguridad, estar por encima de los intereses particulares de cada uno de los elementos del ecosistema, incluir a los actores e intereses públicos y privados, establecer prioridades, financiar líneas de actuación e impulsar la gobernanza del ecosistema de seguridad. Para comenzar la transición, se debería valorar la figura de un Alto Comisionado de Ciberseguridad en la Presidencia del Gobierno.

Diferenciación de las culturas PIC y NIS

La seguridad PIC y la ciberseguridad NIS ocupan ámbitos de actuación diferentes, tal y como reconoce la Directiva NIS (seguridad nacional frente a seguridad económica). El alcance y planteamientos vinculados a la seguridad de las redes y sistemas de información requiere una aproximación (económica) que es sustancialmente distinta a la seguridad física. En la regulación gubernamental de las infraestructuras críticas ha prevalecido el enfoque de la seguridad, pero ahora que la ciberseguridad se ha ampliado al ámbito de la seguridad económica debería equilibrarse con un enfoque de oportunidades. La trasposición de la Directiva NIS debería haber servido para diferenciar y complementar ambos enfoques, pero la elaboración del RD 12/2018, sin participación privada, ha perpetuado el enfoque de seguridad, y su desarrollo reglamentario podría acentuar más su hegemonía.

La necesidad de diferenciar y complementar ambas culturas se evidencia en el desdoblamiento de las mesas del CNPIC: una para la protección física de las

[10] También parece necesario articular foros de confianza donde puedan colaborar las empresas, y estas con la Administración, cuando se observan situaciones anómalas para gestionarlas antes de entrar en gestión de crisis. Los ejercicios ayudan, pero hay que programarlos para que cubran más sectores de actividad.

[11] En línea con la lógica seguida por la Comisión de revisar el estatuto y funciones de Enisa en la UE o del Gobierno británico con el National Cyber Security Centre (NCSC), entre otros.

infraestructuras críticas (cultura PIC) y otra para los aspectos de ciberseguridad de esas infraestructuras. La diferenciación de ambas culturas ha permitido progresar la colaboración público-privada en el sector de las infraestructuras críticas, pero esa diferenciación debería ser mayor en los sectores de las redes y sistemas de información (cultura NIS).

La prevalencia de la cultura PIC hace que, por ejemplo, el reporte de incidentes en el ámbito PIC dependa del nivel de alerta en el que se encuentra la seguridad (física) nacional, la cual no siempre guarda relación directa con el nivel de riesgo o alerta en el ámbito de la ciberseguridad. En el mismo sentido, la autoridad de control no coincide con el CERT de referencia (por ejemplo, en Renfe la autoridad de control es el CNPIC; sin embargo, el CERT de referencia es el CCN-CERT). Finalmente, dada la indefinición de la figura del CISO en el RD 12/2018[12], se corre el riesgo de que se acabe regulando un perfil de responsable de seguridad de la información (CISO) que permita el intrusismo de perfiles de seguridad física aprovechando la regulación ministerial (Interior) de las figuras del director de Seguridad o del responsable de Seguridad y Enlace. La necesidad de diferenciar ambas culturas es también evidente en el ámbito del sector público (Interior), donde se necesitaría contar con más personal formado en la cultura de la seguridad de la información para facilitar la interacción entre los actores públicos y privados en materia de ciberseguridad (por ejemplo, en materia de denuncia de delitos telemáticos[13]).

Por consiguiente, la ECN de 2019 debe diferenciar ambas culturas y evitar la expansión de la cultura PIC de seguridad nacional a los nuevos ámbitos de la seguridad económica distintos de las infraestructuras críticas. La diferenciación es ineludible en el ámbito NIS, regulado por el RD 12/2018, y lo será más en relación con los sistemas de información y tecnologías que son soporte de la operación industrial (OT e IIoT[14]), que difieren en requisitos, ámbito de aplicación y grado de madurez en relación con los elementos utilizados en entornos IT.

Regulación de las obligaciones empresariales sobre ciberseguridad

La ECN debe liderar la consolidación de la ciberseguridad dentro del tejido empresarial complementando las medidas adoptadas para proteger la seguridad física y la continuidad de los sistemas digitales de información con otras diseñadas para un nuevo

[12] "Los operadores de servicios esenciales designarán y comunicarán a la autoridad competente, en el plazo que reglamentariamente se establezca, la persona, unidad u órgano colegiado responsable de la seguridad de la información, como punto de contacto y de coordinación técnica con aquella. Sus funciones específicas serán las previstas reglamentariamente" (art. 16.3).

[13] El sector privado es consciente de las limitaciones de medios y personal de la Administración para atender las crecientes tareas de ciberseguridad; por eso insiste en la necesidad de centralizar medios y recursos para evitar su dispersión y duplicación.

[14] Los componentes OT, aunque generalmente son muy fiables, carecen en su mayoría de una ciberseguridad por diseño (la capa de seguridad se añade posteriormente). Es necesario evolucionar hacia una ciberseguridad OT, IT e IoT por diseño, homologada por terceros de confianza, lo que supone una ampliación de la ciberseguridad hacia lo que se conoce con distintas denominaciones según las fuentes: *seguridad integral*, *seguridad digital*, *seguridad 360º*…
(cont.)

escenario global de gestión integrada que demanda una visión integral y anticipativa de la función de seguridad.

Esto implica que las empresas deben consolidar y unificar el perímetro de la gobernanza de la seguridad, extenderlo al ámbito internacional y fomentar la ciberinteligencia con alcance global (internacional), así como una mayor implicación en las relaciones con las instituciones locales en materia de gobernanza y colaboración público-privada[15].

Esta nueva concepción de la ciberseguridad como parte integrada de la seguridad digital consolida con un enfoque holístico la gestión de riesgos de los distintos niveles de la seguridad, físicos y lógicos, para el aseguramiento de las operaciones de la empresa, desde la ciberseguridad IT y OT hasta la inteligencia, la protección de activos y la resiliencia, con la visión finalista global sobre la capacidad de recuperación ante incidentes, lo cual exige establecer una capa de gobierno en las empresas.

Es importante incidir en que la seguridad de las empresas no sólo conlleva una actividad operativa y tecnológica sobradamente reconocida el ámbito de la ciberseguridad, sino que es fundamentalmente una competencia relacionada con la aplicación de procedimientos, controles y métodos en torno a la gestión integral de riesgos de seguridad y gestión de crisis.

Para ello, el sector privado coincide en la necesidad de generalizar el cumplimiento de unas medidas razonables de ciberseguridad a todas las empresas que participan en la cadena de suministro de la ciberseguridad, al igual que se ha generalizado la aplicación del Reglamento General de Protección de Datos (RGPD) en el ámbito de la privacidad. La regulación contendría medidas de estímulo (certificación aprobada, rebaja de sanciones, buenas prácticas) y penalización (exclusión de licitaciones públicas o subvenciones, multas).

El sector privado entiende que la regulación debe ser escalable en función de la relevancia de cada empresa para la seguridad nacional o la seguridad económica (**no se puede exigir lo mismo a todas las empresas**). La regulación debe ser elaborada en comunicación con el sector privado cuando afecta a su actividad empresarial, tecnológica o industrial (**el ecosistema debe participar en la regulación**). La regulación debe establecer el marco general de control en cuestiones como la organización, condiciones, responsabilidades o buen gobierno del sector privado (**el qué**), entre otros, pero dejar el cumplimiento al criterio de las empresas (**el cómo**)[16]. El procedimiento de regulación unilateral utilizado hasta ahora por el Sistema de Ciberseguridad Nacional **fomenta la inseguridad jurídica y económica de las**

[15] No hay respaldo legal para exigirlo. No obstante, la normativa no debería imponer perfiles rígidos de responsabilidad al sector privado. El CISO debería tener conocimientos de ciberseguridad y contar con una organización de apoyo especializada, además de poder externalizarse en el caso de las pymes. La voluntariedad fomenta la negligencia de las pymes y pone en riesgo las cadenas de suministro de ciberseguridad.

[16] El Estado delimita el marco de control, evalúa su cumplimiento, emite recomendaciones y marca el plazo para la siguiente evaluación.

empresas, por lo que se debería sopesar la adopción de una Ley de Ciberseguridad Nacional que corrigiera ese riesgo.

De acuerdo con lo anterior, la ECN de 2019 debería incluir, al menos, las siguientes medidas:

- Exigir la aplicación de los principios de privacidad, confidencialidad y ciberseguridad por diseño y la gestión de los riesgos e incidentes de ciberseguridad, siguiendo el modelo NIS, en el diseño y fabricación de los productos o servicios, incluyendo el análisis de riesgo por diseño.

- Exigir la obligación de establecer, aprobar y actualizar periódicamente las estrategias, planes o medidas de ciberseguridad de las empresas y los presupuestos necesarios para ejecutar los planes de transformación establecidos en la estrategia, así como incluir en ésta los planes de concienciación y formación sobre cultura de ciberseguridad —adaptados a los perfiles y funciones de los empleados, alta dirección y el consejo de administración—, de carácter obligatorio y acreditable[17].

- Designar un responsable de seguridad de la información (CISO, CSO) que cubra la ciberseguridad en los ámbitos IT y OT y de los productos y servicios de toda la cadena de suministro. El responsable, interno a la organización o externalizado en un tercero, debería contar con un mandato, funciones y presupuesto asignados por la organización. Este cargo debería contar asimismo con el compromiso y supervisión de la Dirección y ser responsable del gobierno, la elaboración de un plan de riesgos y la gestión integral de la seguridad de la información.

- Obligación de los empleados de informar a la organización de los ciberincidentes para evitar que no se notifiquen incidentes por temor a sanciones de la empresa.

- Implantar el principio de corresponsabilidad entre las empresas que forman parte de la cadena de valor, en particular la corresponsabilidad de invertir en ciberseguridad (p. ej. ámbito industrial OT).

Dependencia tecnológica

Existe un consenso entre el sector privado en valorar que España se encuentra bien situada internacionalmente en lo que respecta a los procedimientos de gobernanza de la ciberseguridad, con el sector privado a través del CNPIC y con las Administraciones Públicas a través del CCN. Sin embargo, se aprecia un claro desequilibrio en lo que atañe a la inversión en tecnologías de ciberseguridad, en particular en la inversión en herramientas informáticas empleadas en los CSIRT, debilidad común a la mayor parte

[17] Hasta ahora, ni siquiera las empresas que cotizan tienen la obligación de presentar ante el consejo de administración una memoria anual sobre su política de ciberseguridad.
(cont.)

de los Estados miembros de la UE en comparación con Estados Unidos, Rusia o China.)[18].

La ECN debe impulsar una I+D+i en materia de ciberseguridad ligada a la demanda y al desarrollo de nuevas tecnologías que potencie el desarrollo de una industria nacional de ciberseguridad. Dado que en el contexto actual es difícil disminuir la dependencia tecnológica de determinadas tecnologías clave como Internet, microprocesadores o tecnologías de cifrado, es necesario reforzar ámbitos de I+D+i alineados con tecnologías clave actuales o a futuro como inteligencia artificial, cadena de bloques, informática cuántica o el Internet industrial de todas las cosas. Ese esfuerzo permitiría desarrollar a nivel nacional esos ámbitos e introducir la ciberseguridad en el diseño de las propias tecnologías desde el principio.

Para corregir esta desviación, la ECN de 2019 debe desarrollar la dimensión tecnológica e industrial de la ciberseguridad. Para ello, la ECN debe impulsar una I+D+i nacional en materia de ciberseguridad ligada a la demanda y desarrollo de nuevas tecnologías (IA, IIPC…) que potencie el desarrollo de una industria nacional de ciberseguridad. También debe aprovechar las oportunidades de I+D+i que se abran en la UE (Horizonte Europa, Fondo de Ciberseguridad) para posicionar el ecosistema español de ciberseguridad dentro del nuevo contexto europeo de ciberseguridad en formación (Ley de Ciberseguridad, Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y Red de Centros Nacionales de Coordinación).

Se necesita ser vigilante respecto al despliegue y uso de tecnologías *hardware* y *software* de fabricantes que estén influenciados directa o indirectamente por sus propios Gobiernos, tal como supuestamente podrían estarlo Kaspersky, Huawei o ZTE, para no comprometer la seguridad o la reputación de la cadena de suministro de las empresas nacionales. El tema adquiere una doble dimensión geopolítica (p. ej. China y Rusia frente a EE. UU. y Europa) y económica (guerra comercial de productos y servicios IT) entre regiones confrontadas. Aun siendo conscientes de las limitaciones nacionales y de la UE para aspirar a una soberanía tecnológica plena, la nueva ECN deberá ampliar la autosuficiencia tecnológica todo lo posible, empezando por lo más crítico, pero sin renunciar a crear una **base tecnológica e industrial nacional de ciberseguridad**, relevante a mayor plazo.

El fomento de esa base nacional (**seguridad tecnológica**) no puede entenderse de forma proteccionista, evitando toda colaboración con terceros, sino fomentándola con aquellos que puedan ser socios estratégicos para el desarrollo mediante acuerdos de cooperación internacional y compartiendo los mismos principios y valores, respetando los derechos y libertades de los ciudadanos y facilitando el acceso a datos almacenados en el extranjero. Tampoco puede entenderse de forma autárquica, sino pragmática: ya que en el contexto actual es difícil disminuir la dependencia en tecnologías claves como Internet, microprocesadores o cifrado, entre otras, es mejor reforzar los ámbitos de I+D+i

[18] Se deben potenciar soluciones nacionales para nichos críticos de seguridad y de negocios para converger las inversiones públicas y las privadas (invertir en los 'agujeros' de ciberseguridad y en los nichos tecnológicos que el mercado no cubre). La ciberseguridad debe integrarse en los planes nacionales de investigación, los programas duales del CDTI y el Horizonte Europa de la UE.

asociados con las tecnologías anteriores o con las futuras (*blockchain*, inteligencia artificial, informática cuántica, Internet de las cosas…).

En consecuencia, es necesario mantener y/o establecer alianzas estratégicas con fabricantes internacionales fiables de *hardware* y *software* internacionales fiables que colaboren con el desarrollo de un tejido profesional y empresarial local. Igualmente, es necesario apoyar a las empresas nacionales para que inviertan en sus proyectos de I+D+i y generen así productos y servicios que compitan de manera eficaz a nivel internacional. Corresponde a la ECN fomentar alianzas estratégicas con Gobiernos y empresas internacionales, la implementación de programas educativos encaminados al desarrollo de herramientas de última generación en materia de ciberseguridad, la inversión y/o incentivos a la inversión en el desarrollo de productos y servicios nacionales que sean competitivos a nivel internacional para impulsar la adopción de tecnología nacional.

En particular, es necesario esforzarse en disminuir la dependencia de determinadas tecnologías claves (por ejemplo, en materia de cifrado o inteligencia artificial) mediante el desarrollo desde el sector privado nacional del negocio de la ciberseguridad, ofrecida a la Administración Pública en un marco común de colaboración público-privada. El reto es fomentar la ciberseguridad tanto del lado de la demanda como del de la oferta.

La ECN de 2019 debe promover la creación de un ecosistema nacional de empresas y desarrollarlo mediante programas de educación, incentivos a la inversión local y acuerdos internacionales para el desarrollo de talento en materia de inteligencia artificial, IoT y su relación con la ciberseguridad que permitan generar en España productos y servicios que compitan a nivel internacional. Tanto en el mercado nacional como en el global, se deben desarrollar empresas que produzcan ciberseguridad en lugar de empresas que la consuman.

De la misma manera, la ECN de 2019 debe fomentar, por un lado, la generación de datos de alta calidad (mediante el despliegue de sensores seguros, fiables y veraces) y la rápida adopción de tecnología como la inteligencia artificial con fines propios de seguridad. También debe articular mecanismos por los cuales se informe de manera privada a los fabricantes de *hardware* y *software* sobre las vulnerabilidades que sean detectadas en sus productos y que representen un riesgo de ciberseguridad para evitar la explotación ilegítima de estas vulnerabilidades.

Certificación de productos y servicios

Para afrontar la dependencia tecnológica sería preciso, entre otras medidas, establecer una certificación específica de determinados productos particularmente sensibles por la función que desempeñan en las redes y sistemas de información. En la actualidad no se dispone de la infraestructura apropiada para ello y el esquema de certificación es inviable desde el punto de vista económico[19]. Debería ser viable, por ejemplo, una certificación de productos de nicho cuya aplicación sea crítica en las comunicaciones

[19] La certificación *total* es técnicamente imposible, limitada en el tiempo y demasiado cara. La aportación de Enisa es en la actualidad insuficiente. Podría elaborarse algo similar a una ISO que establezca los requisitos de seguridad y los mecanismos de verificación.

gubernamentales o por la función que desempeñan en el núcleo de redes de telecomunicaciones. Lo mismo podría decirse respecto de las cadenas de suministro asociadas a la ciberseguridad cuando las empresas no disponen de la tecnología necesaria para hacerlo o no existen proveedores que cumplan las especificaciones mínimas de ciberseguridad en los ámbitos IT, OT e IIoT. Asimismo, existen empresas que ofrecen servicios esenciales de infraestructuras críticas proclives a establecer esquemas de certificación de obligado cumplimiento.

En el caso de productos y servicios IT de uso general, la Administración debería establecer niveles o compromisos y garantías de seguridad a través de certificaciones tipo ISO y dejar en manos del sector privado la forma técnica de instrumentalizarlo. La certificación de estos esquemas de seguridad por terceros ofrecería un alto nivel común de seguridad a la Administración Pública.

En todos los casos, es determinante el plazo establecido para la definición, alcance y aprobación de los esquemas de certificación. En este sentido, los estándares ISO, al ser consensuados, demandan plazos muy prolongados (unos 5 años), lo cual lleva a su revisión y actualización tras ser aprobados. Sin embargo, otros organismos (como, por ejemplo, Enisa) acortan el plazo, aunque no siempre cuenten con el consenso de todos los agentes.

Capacitación y formación

Existe una brecha importante entre los recursos humanos disponibles y los demandados en materia de ciberseguridad, tanto en el sector privado como en el público. Resulta necesario adecuar las herramientas de formación/training a cada etapa educativa y profesional para desarrollar una sociedad formada por ciudadanos educados en ciberseguridad en su vida diaria y por profesionales formados en la ciberseguridad empresarial, además de por profesionales de ciberseguridad entrenados apropiadamante en herramientas de prevención, detección y resolución de ciberataques

El empleo de los fondos asignados a la formación resulta en general ineficiente, ya que carecen de continuidad en el tiempo y los mecanismos de evaluación son ineficaces, razón de más para exigir la obligatoriedad y el cumplimiento en la empresa de estos programas de formación para consolidar la concienciación y formación de los empleados.

La importancia de promover una cultura de ciberseguridad en los ámbitos empresariales y educativos obliga a fomentar el empleo de herramientas formativas y de simulación adecuadas a cada etapa (simuladores y entornos de RV/RA para la educación, *cyber ranges* de diferentes características según los destinatarios) con el fin de preparar a las nuevas generaciones para el reto de la ciberseguridad y las tecnologías disruptivas asociadas.

Colaboración público-privada

La colaboración público-privada ha funcionado bien mientras se desarrollaba la protección de las infraestructuras críticas en las que ambos sectores compartían intereses y criterios, aunque no en condiciones de igualdad. La colaboración no cuenta

con un marco institucional reglado como los de otros países (Agencia Nacional de Ciberseguridad Francesa, ANNSI) y el sector privado está excluido del proceso de decisiones del Consejo de Ciberseguridad Nacional, de la elaboración de las estrategias de ciberseguridad nacional y de la regulación y desarrollo normativo de la ciberseguridad[20]. Sin embargo, la evolución y ampliación de la ciberseguridad tiende a diferenciar las posiciones de ambos sectores, y la ECN de 2019 debería articular un sistema de colaboración.

La revisión de la ECN ofrece una oportunidad para regular, sistematizar y dinamizar la colaboración. La colaboración público-privada tiene dos vertientes: la participación en el proceso de decisiones y en la evaluación de la colaboración. La primera se puede garantizar a través de su **presencia reglada** en los distintos niveles de gestión y la segunda mediante **mecanismos de revisión** que permitan a ambas partes evaluar el desempeño de la colaboración[21]. La revisión de la ECN debería atender a ambas vertientes, ya que hasta ahora no existen protocolos vinculantes para la participación, fijación de objetivos, supervisión del cumplimiento y evaluación de la cooperación público-privada.

Sería recomendable la formación de foros, mesas o grupos de trabajo abiertos a la participación de asociaciones empresariales y empresas del sector en los que el sector privado tuviera capacidad de iniciativa para plantear propuestas de búsqueda de convenios o acuerdos de cooperación. En el mismo sentido, la ECN de 2019 podría proponer la elaboración de un libro blanco de la cooperación público-privada en materia de ciberseguridad que cubriera un amplio espectro de cuestiones (investigación, intercambio de datos e inteligencia, vulnerabilidades, atribución, supervisión, cifrado, deber de asistencia pública, defensa activa y umbrales de responsabilidad, entre otros) y dispusiera de un sistema de indicadores para evaluar el progreso y el impacto de la cooperación público-privada en los distintos ámbitos.

En tanto no se regule la participación del sector privado, se pueden repetir situaciones perjudiciales como la ocurrida con la trasposición de la Directiva NIS —en la que las iniciativas gubernamentales llegaron a conocimiento del sector privado en fase de consulta pública— o la que ha ocurrido con su desarrollo reglamentario —en el que el sector privado no ha participado en la regulación de asuntos tales como la función del responsable de seguridad de la información[22]—. La regulación permitirá al conjunto de los agentes del sector privado definir sus representantes y mecanismos de interlocución con los organismos públicos.

Otro aspecto que considerar, dado el incremento constante de ciberataques, es definir y regular los mecanismos de respuesta, incluida la defensa activa en los sectores público y privado. Como resalta ECSO, los instrumentos de detección y respuesta están

[20] La Administración considera los contactos informales en estos procesos con alguna empresa o con expertos a título individual como una muestra de la cooperación público-privada y sigue sin regular la participación estructurada del sector privado en las decisiones que lo afectan.

[21] Obligación de vincular cada objetivo de la ECN con unas metas y un conjunto de indicadores de cumplimiento para evaluar el grado de avance.

[22] Parece que el perfil y las funciones de la entidad responsable de la seguridad creados en el RD 12/2018 se están desarrollando sin participación privada.

menos desarrollados que los de prevención y protección, pero la responsabilidad de su desarrollo corresponde al Estado. La defensa pasiva frente a cualquier tipo de ataque representa una carga económica soportable para pocas empresas, por lo que corresponde al sector público elevar los niveles de disuasión adoptando **medidas de defensa activa** y consolidando instrumentos de ciberdiplomacia y ciberdefensa en situaciones de particular gravedad. En la misma idea de segmentar las capacidades y responsabilidades de ciberseguridad entre los sectores público y privado, corresponde al sector público encargarse de las **certificaciones críticas** relacionadas con la seguridad de las cadenas de suministro, porque las empresas carecen de los medios técnicos para hacerlo. Finalmente, la Administración debe facilitar los **procesos de denuncia** de delitos telemáticos para evitar las dificultades actuales[23].

La colaboración público-privada se extiende a un ecosistema formado, junto con las Administraciones —del Estado y las autonomías— y las empresas, por centros tecnológicos, universidades, centros de investigación, asociaciones y fundaciones, entre otros, cuyo potencial sinérgico se debería potenciar en la revisión de la ECN. La **potenciación del ecosistema** mejoraría su madurez y facilitaría economías de escala en la inversión pública y privada, nacional y europea, además de canalizar esa inversión hacia líneas estratégicas de actuación protegiendo la industria de la ciberseguridad nacional, desarrollando la I+D+i, consolidando la oferta y potenciando la producción y comercialización de productos y servicios nacionales[24]. La coordinación del ecosistema facilitaría atender los intereses de ciberseguridad de la empresa privada, orientados a las necesidades generales y demanda del mercado, con el apoyo selectivo de la Administración hacia nichos de mercado vinculados a la **protección de vulnerabilidades** críticas de relevancia estratégica, pero que carecen de mercado potencial y no son atractivos para su industrialización (p. ej. el desarrollo de criptosistemas). En el mismo sentido, la coordinación del ecosistema debe orientarse a fomentar acuerdos internacionales y asociaciones estratégicas con países y empresas fiables y con fuentes de financiación externas, como por ejemplo el programa Horizonte Europa.

Conclusiones

La revisión de la Estrategia de Ciberseguridad Nacional de 2013 es una buena oportunidad para incluir en su elaboración a la mayor parte posible de implicados. Sólo una amplia participación del sector público y privado (*whole-of-nation approach*) daría a la Estrategia un carácter inclusivo y "nacional" (Estrategia *Nacional* de Ciberseguridad), mientras que una participación restringida a la Administración (*whole-of-government approach*) limitaría su alcance al gubernamental (Estrategia de Ciberseguridad Nacional).

[23] En la actualidad, la Oficina de Coordinación PIC indica a la empresa denunciante, caso a caso, si corresponde a la Policía Nacional o la Guardia Civil la tramitación de una denuncia dada. Las FCSE carecen de los medios y procedimientos adecuados para atenderlas y obligan a desplazamientos innecesarios y a identificar la IP.

[24] Esta red, liderada por Incibe y miembro de ECSO, no cuenta con fondos propios, sistematización ni proyecto (salvo reuniones). Un mayor apoyo institucional al CSIRT.es, aprovechando su capacidad de colaboración público-privada en el campo de respuesta a incidentes.

Este documento se ha elaborado entre los miembros del Grupo de Trabajo de Ciberpolítica que pertenecen al sector privado para que puedan utilizar libremente sus conclusiones todas las personas implicadas en la elaboración o la realización de propuestas para la Estrategia.

La Estrategia de Ciberseguridad Nacional de 2013 puso en marcha una colaboración público-privada que ha funcionado bien y ha generado confianza entre ambos sectores a propósito de la seguridad nacional en general y especialmente en relación con las infraestructuras críticas. Lo que estas propuestas pretenden es que la nueva Estrategia amplíe esa buena relación a otros ámbitos distintos de la seguridad nacional y que afectan a las oportunidades del ciberespacio para las empresas en cuestiones que pertenecen a la seguridad económica.

Para el buen funcionamiento del nuevo modelo de relación público-privada y facilitar su obligada regulación por el sector público, es necesario que el sector privado se organice para ofrecer una interlocución única. Estas propuestas para la revisión de la Estrategia de Ciberseguridad Nacional son una modesta iniciativa para fomentar esa organización.