La revisión de la Estrategia de Ciberseguridad Nacional: una visión desde el sector privado

Javier Alonso Lecuit | Miembro del Grupo de Trabajo sobre Ciberpolítica del Real Instituto Elcano

Tema

El sector privado se juega mucho en la revisión de la Estrategia de Ciberseguridad Nacional de 2013. No sólo tiene que hacer frente a la creciente naturaleza, complejidad y gravedad de las ciberamenazas, sino que también se ve afectada económicamente por la mayor parte de sus líneas de acción.

Resumen

La Estrategia de Ciberseguridad Nacional (ECN) de 2013[1] se encuentra en revisión. Ésta responde a tres consideraciones: la adaptación de la ECN a un nuevo contexto de retos y tecnologías de ciberseguridad inexistentes en 2013, la aplicación de las medidas destinadas a garantizar un nivel común de seguridad en las redes y los sistemas de información exigido en la Directiva NIS[2] y las mejoras en la ECN a partir de la experiencia obtenida desde 2013.

Este ARI resume las perspectivas del sector privado sobre esos tres aspectos, que se desarrollan con más detalle en el Documento de Trabajo del mismo título elaborado dentro del Grupo de Trabajo sobre Ciberpolítica del Real Instituto Elcano.

Análisis

Adaptación al nuevo contexto

Para adaptarse a los nuevos retos, la futura ECN habrá de añadir entre sus actuales objetivos, centrados en la ciberseguridad IT, los desafíos vinculados al proceso de la transformación digital, en particular aquellos derivados de la digitalización de entornos industriales (industria 4.0), la seguridad industrial operativa (OT), la seguridad de los dispositivos conectados (IIoT e IoT) y el uso de tecnologías avanzadas en el ámbito de la ciberseguridad, tales como la inteligencia artificial, *big data*, computación cuántica o esquemas de cifrado cuántico.

Igualmente será necesario que la ECN de 2019 preste el apoyo que el sector privado necesita en materia de ciberinteligencia y apoyo operativo coordinado para hacer frente

[1] Estrategia Nacional de Ciberseguridad, 2013.

[2] Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

a ciberataques de gran impacto, así como amenazas híbridas promovidas desde terceros Estados y ejecutadas por organizaciones del cibercrimen, cuya respuesta puede sobrepasar las capacidades individuales tecnológicas y operativas del sector privado.

La ampliación del espectro de riesgos obliga a reforzar el enfoque preventivo sobre la base de una nueva regulación de las obligaciones empresariales relativas a la ciberseguridad —similar a la establecida con éxito en la protección de datos de carácter personal (LOPDGDD[3])— implantando la ciberseguridad por diseño como requisito obligatorio de la compra pública de bienes, instalaciones e infraestructuras y en todas las empresas que participan en las cadenas de suministro. Esta regulación deberá establecer un marco general de control en cuestiones como la organización, responsabilidades o buen gobierno del sector privado, entre otros, y dejar al criterio de las empresas el modo de llevar a cabo su cumplimiento, guardando la debida proporcionalidad con la relevancia de cada empresa para la seguridad nacional o la seguridad económica —es decir, evitando exigir lo mismo a todas las empresas— y contando desde su inicio con la participación del sector privado en cuanto afecte a su actividad empresarial, tecnológica e industrial para evitar procesos de regulación unilateral.

En línea con lo anterior, la ECN de 2019 debería exigir a las empresas, entre otras obligaciones, las siguientes. Primero, aplicar los principios de privacidad, confidencialidad, ciberseguridad por diseño y gestión de los riesgos e incidentes de ciberseguridad en el diseño y fabricación de los productos o servicios, incluyendo el análisis de riesgo por diseño. En segundo lugar, la obligación de establecer, aprobar y actualizar periódicamente las estrategias, planes y medidas de ciberseguridad de las empresas y los presupuestos necesarios para ejecutar los planes de transformación establecidos en la estrategia, incluyendo en ésta los planes de concienciación y formación —de carácter obligatorio y acreditable— sobre cultura de ciberseguridad, adaptados a los perfiles y funciones de los empleados, alta dirección y consejo de administración. Tercero, integrar a través de un comité, órgano de gobierno o persona la figura del CSO (*chief security officer*), sobre cuya figura recaen, entre otras, las responsabilidades de ciberseguridad en los ámbitos IT y OT y de productos y servicios de toda la cadena de suministro. Cuarto, implantar el principio de corresponsabilidad entre las empresas que forman parte de la cadena de valor y suministro, en particular la corresponsabilidad de invertir en ciberseguridad.

Exigencias establecidas en la Directiva NIS

La adaptación de la ECN de 2013 a las exigencias establecidas en la Directiva NIS y su transposición al RDL 12/2018[4] obliga a modular el enfoque de la seguridad de las 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. El sector privado considera que la cultura de

[3] Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de derechos digitales.

[4] Real Decreto Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

(cont.)

infraestructuras críticas (ley PIC y real decreto de desarrollo de 2011[5]), vinculada a la seguridad física, ha predominado en la definición de la ECN de 2013 y está aprovechando el RDL 12/2018 para ampliar su ámbito de actuación más allá de lo dispuesto en la Directiva NIS. De no corregirse esta tendencia, los responsables procedentes de la seguridad física podrían acabar ocupando los puestos de responsables de seguridad de la información IT (art. 16.3 del RDL 12/2018) y los relacionados con la ciberseguridad OT e IIoT, es decir, el nuevo perímetro de la seguridad digital.

En el mismo sentido, el incremento en número y la aceleración en el tiempo de los cambios tecnológicos, unidos a los nuevos marcos regulatorios y a la proliferación de relaciones institucionales, desborda la capacidad de gestión del modelo actual de coordinación. En consecuencia, el sector privado considera necesario, por una parte, centralizar el sistema de ciberseguridad nacional en aquellos aspectos relacionados con el núcleo de la seguridad nacional y el sector público, de forma que se refuercen las competencias de coordinación de las autoridades. Por otra parte, el sector privado plantea como línea de actuación prioritaria la creación de una Agencia de Ciberseguridad con el objetivo de abarcar la complejidad e importancia que está alcanzando la ciberseguridad por encima de los intereses particulares de cada uno de los agentes 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 iniciar esta transición, se propone considerar la figura de un Alto Comisionado de Ciberseguridad en la Presidencia del Gobierno.

Valoración y mejoras de la ECN de 2013

La valoración de la experiencia obtenida de la ECN de 2013 es, en conjunto, positiva, aunque la ECN de 2019 precisa mejoras significativas en varios aspectos. 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 (hasta la fecha carentes de trasparencia), sino de su cumplimiento, por lo que será necesario respaldar en la ECN de 2019 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 próxima ECN.

Segundo, la cooperación público-privada sigue sin la regulación prevista en la Ley de Seguridad Nacional (art. 7). El sector privado no participa en todas las decisiones que lo afectan y la regulación se presenta como un hecho consumado. La revisión debería regular, sistematizar y dinamizar la colaboración público-privada en dos vertientes: la participación en el proceso de decisiones y en la evaluación de la colaboración. La primera se puede garantizar mediante su presencia reglada en los distintos niveles de

[5] Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, y Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

gestión y la segunda mediante mecanismos de revisión que permitan evaluar el desempeño en la colaboración por ambas partes.

La colaboración público-privada se extiende a un ecosistema formado por las Administraciones del Estado y de las autonomías, las empresas y los centros tecnológicos, universidades, centros de investigación, asociaciones y fundaciones, entre otros, cuyo potencial sinérgico se debería potenciar en la revisión de la ECN. La gobernanza actual del sistema de ciberseguridad nacional no abarca el ecosistema mencionado y limita la coordinación del presidente del Consejo de Ciberseguridad Nacional al sector gubernamental, por lo que la ECN de 2019 podría mejorar la gobernanza e inclusividad del sistema si dotara al presidente 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.

Otro aspecto que considerar es definir y regular los mecanismos de respuesta, incluida la defensa activa, en los sectores público y privado dado el incremento constante y la gravedad de los ciberataques. La defensa exclusivamente pasiva representa una importante carga económica, por lo que corresponde al sector público elevar los niveles de disuasión adoptando medidas de defensa activa y consolidando instrumentos de ciberdiplomacia y la ciberdefensa en situaciones de particular gravedad. Del mismo modo, corresponde al sector público establecer las certificaciones críticas relacionadas con la seguridad de las cadenas de suministro, dado que las empresas carecen de los medios técnicos para hacerlo.

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 las disrupciones ocasionadas por la tecnología en el ámbito de la seguridad. En particular, la ECN de 2019 deberá potenciar una base tecnológica e industrial nacional de ciberseguridad mediante programas específicos de investigación, desarrollo, innovación (I+D+i) y adquisiciones, así como fomentar acuerdos internacionales que faciliten a la industria nacional el acceso a tecnología y mercados. 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 del negocio de la ciberseguridad desde el sector privado nacional, ofrecido a la Administración Pública en un marco común de colaboración público-privada.

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. La ECN ha de promover el desarrollo de empresas que producen ciberseguridad en lugar de empresas que la consuman, tanto en el mercado nacional como en el global.

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 o respecto a las cadenas de suministro asociadas a la ciberseguridad cuando las empresas no disponen

de la tecnología necesaria para hacerlo o no existan proveedores que cumplan las especificaciones mínimas de ciberseguridad en los ámbitos IT, OT e IIoT. En este sentido, existen empresas que ofrecen servicios esenciales de infraestructuras críticas proclives a establecer esquemas de certificación de obligado cumplimiento.

En relación con la capacitación y formación, existe en la actualidad una brecha importante entre los recursos humanos disponibles y los demandados en materia de ciberseguridad, tanto en el sector privado como en el público. Deberían reforzarse, con el impulso de la Administración, los programas de capacitación, concretados en programas educativos de aplicación a colegios y a la formación profesional, encaminados a dinamizar el mercado de talento, y exigir la obligatoriedad y el cumplimiento de programas de formación en la empresa para consolidar la concienciación y formación de los empleados.

Conclusiones y propuestas planteadas por el sector privado

A continuación, se comparan los objetivos, principios y líneas de acción de la ECN establecidos en 2013 (columna de la izquierda) con las propuestas planteadas por el sector privado que tienen como finalidad concretar, modificar y añadir las propuestas a la ECN de 2019 que se recogen en las tablas siguientes (columna de la derecha).

Objetivos de la ECN

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	La ciberseguridad es trasversal. 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)
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	Las infraestructuras críticas son una parte de la ciberseguridad y no al revés. 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)
V	Sensibilizar a los ciudadanos, profesionales, empresas y Administraciones Públicas españoles de los riesgos derivados del ciberespacio	De la concienciación al compromiso. 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
VI	Alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita España para sustentar todos los objetivos de ciberseguridad	Soberanía tecnológica. 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

Principios rectores de la ECN

Principios	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	Centralización del Sistema de Ciberseguridad 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 Creación de una Agencia de Ciberseguridad. 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
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 participación privada es obligatoria según la Ley de Seguridad Nacional y debe regularse. 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

Principios	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	Definición y capacitación de los responsables públicos y privados. 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 La participación privada complementa, pero no reemplaza, a la pública en las funciones de seguridad nacional. 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
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	Dotar a la cooperación internacional de una dimensión de inteligencia económica. 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

Líneas de acción de la ECN

	ECN 2013	ECN 2019
1	Capacidad de prevención, detección, respuesta y recuperación ante las ciberamenazas	Llegar donde la capacidad privada no llega. 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
2-3	Seguridad de los sistemas de información y telecomunicaciones que soportan las Administraciones Públicas y las infraestructuras críticas	Mecanismo de evaluación. 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
4	Capacidad de investigación y persecución del ciberterrorismo y la ciberdelincuencia	La colaboración debe ser de doble sentido. 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
5	Seguridad y resiliencia de las TIC del sector privado	Ventanilla única, procedimientos pactados, denuncias y retroalimentación. Centralizar, consensuar y simplificar la colaboración público-privada Implantar una infraestructura de certificación concertada con el sector privado
6	Conocimientos, competencias e I+D+i	Sin presupuestos ni estrategias de inversión no hay políticas de I+D+i. Dedicar parte del presupuesto de ciberseguridad nacional a preservar la base tecnológica e industrial de la ciberseguridad 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 Partenariados. 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

Líneas de acción adicionales a las adoptadas en la ECN 2013

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	**La ciberseguridad es un activo estratégico.** 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. **Todos rinden cuentas y más cuanta más relevancia tienen para la ciberseguridad.** 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.
2	Evitar la hiperregulación unilateral del sector público	Para ello es necesaria la **implicación del sector privado tanto en España como en la UE** desde los primeros momentos en el proceso regulatorio que lo afecte. **La norma fija el qué y las empresas el cómo.** 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.
3	Dotación presupuestaria independiente como cualquier otra política pública.	**Sin presupuesto no hay política.** La ECN deberá acompañarse de una memoria económica con los distintos objetivos de gasto y su distribución. **Sin supervisión tampoco.** 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.