La nueva Estrategia de Ciberseguridad de 2019

Félix Arteaga | Investigador principal de Seguridad y Defensa del Real Instituto Elcano y coordinador del Grupo de Trabajo sobre Ciberpolítica

Tema

El Consejo de Seguridad Nacional ha aprobado en abril de 2019 una nueva Estrategia de Ciberseguridad que actualiza la de 2013. En conjunto, representa un avance sobre la anterior, aunque su desarrollo dependerá del respaldo político y presupuestario del futuro Gobierno.

Resumen

El Consejo de Seguridad Nacional ha aprobado el 26 de abril de 2019 una nueva Estrategia de Ciberseguridad que actualiza la de 2013. Elaborada por el Consejo de Ciberseguridad Nacional, la nueva Estrategia presenta notables avances sobre la anterior, aunque su aportación final dependerá del respaldo político y presupuestario del futuro Gobierno para desarrollarla. En este ARI se analiza su contenido y se compara con las recomendaciones propuestas desde el sector privado.

Análisis

El Consejo Nacional de Ciberseguridad ha elaborado una nueva Estrategia que actualiza la Estrategia de Ciberseguridad Nacional de 2013[1]. En su diseño y redacción sólo han intervenido representantes gubernamentales del mencionado Consejo a partir de otoño de 2018 y su borrador final quedó listo en febrero de 2019[2]. El sector privado no ha participado en el proceso de elaboración, aunque su borrador final se dio a conocer a expertos a título individual y restringido antes de su publicación. Para dar a conocer la opinión del sector sobre el proceso de revisión en curso, el Grupo de Trabajo de Ciberpolítica del Real Instituto Elcano elaboró unas propuestas para que se incluyeran en la futura redacción[3].

[1] Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional. BOE nº 103 de 30 de abril de 2019, https://boe.es/boe/dias/2019/04/30/pdfs/BOE-A-2019-6347.pdf

[2] En su comparecencia ante la Comisión Mixta de Seguridad Nacional, el secretario de estado y director del Centro Nacional de Inteligencia, confirmó que: "La estrategia, si Dios quiere, en la próxima reunión del Consejo de Seguridad Nacional se presentará para su aprobación porque está ya escrita. No tiene muchos cambios". Diario de Sesiones del 14 de abril de 2019, p. 20, http://www.congreso.es/public_oficiales/L12/CORT/DS/CM/DSCG-12-CM-131.PDF

[3] "Propuestas desde el sector privado para la revisión de la Estrategia de Ciberseguridad Nacional", DT 472019, Real Instituto Elcano, http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/dt4-2019-alonsolecuit-propuestas-sector-privado-revision-estrategia-ciberseguridad-nacional.

Como se verá en la comparación que se va a realizar a continuación, la Estrategia recoge bastantes de esas recomendaciones, lo que refleja la gran coincidencia de perspectivas e intereses entre los sectores público y privado. Las divergencias obedecen a que los representantes del Consejo Nacional de Ciberseguridad (el Sistema de ahora en adelante) están más preocupados por los riesgos y la inseguridad del ciberespacio que por el impacto que puedan tener sobre la actividad económica e industrial del sector privado. Esta preferencia es lógica, dada la competencia exclusiva del sector público en cuestiones de seguridad nacional. Sin embargo, esa reserva competencial se quiebra cuando las decisiones adoptadas abandonan el ámbito restringido de la seguridad nacional y entran el más amplio de seguridad económica.

La Estrategia sólo se limita a emitir unas directrices generales y técnicas a las que tendrán que seguir decisiones políticas concretas para ejecutar las líneas de actuación recogidas en ella. Corresponde al Gobierno respaldar o no al Consejo Nacional de Ciberseguridad en la ejecución de esas medidas, aportando el respaldo político y presupuestario que precisan. Por eso, y desde el sector privado, se proponía que la nueva estrategia anticipara las medidas a desarrollar como la regulación de la participación privada, la necesidad de contar con una memoria económica o la defensa activa, entre otras. La nueva Estrategia recoge alguna de esas propuestas, pero el Gobierno tendrá que definir otras, como su contribución presupuestaria, para que el Plan de Acción con el que se desarrolle la Estrategia cuente con objetivos y recursos concretos y no sólo con buenos propósitos.

Entre las orientaciones a desarrollar sobresale la de regular la cooperación público-privada. La articulación de un foro de Ciberseguridad Nacional (el Foro de ahora en adelante) representa una directriz importante en la nueva Estrategia y responde a la demanda del sector privado. La cooperación entre ambos sectores ha funcionado bien en relación con la protección de las infraestructuras críticas y debería hacerlo a medida que la ciberseguridad se expande por el ámbito de la seguridad económica, la seguridad industrial, los servicios no esenciales y la educación. Para mejorar la colaboración público-privada, se debe mejorar la cooperación pública-publica, reduciendo el número de interlocutores gubernamentales, y se debe articular -la inexistente- cooperación privada-privada, para que el sector gubernamental cuente con una interlocución única e integrada.

La corresponsabilidad como principio

La nueva Estrategia entiende que el ciudadano es “corresponsable” de la ciberseguridad nacional. Su parte de la responsabilidad obedece a que su comportamiento puede influir en la seguridad del ciberespacio, por lo que se le pide que tome conciencia de los riesgos que corre (cultura de ciberseguridad) y se comprometa en la tarea común de proteger a la sociedad, impulsando aquellas medidas que conduzcan a la “necesaria” cooperación para la seguridad común. La necesidad de esta cooperación impuesta puede ser excesiva si, por ejemplo, la carga de la ciberseguridad recae exclusiva o mayoritariamente sobre el sector privado. Incluso si fuera equitativa, la movilización de los ciudadanos ante un peligro colectivo no puede seguir el patrón del extinto servicio militar obligatorio, en el que los ciudadanos sólo tenían el deber de contribuir, sino en el

moderno de corresponsabilidad de las sociedades avanzadas donde actores públicos y privados comparten decisiones, obligaciones y derechos.

Si la responsabilidad es compartida, la cooperación no puede funcionar sólo en apoyo del sector público. El reparto de responsabilidades, lo que corresponde al sector público y al privado no puede ser igual sino asimétrico: mayor peso del sector público en las decisiones que afectan a la seguridad nacional y mayor peso del sector privado en las que afectan a su seguridad económica, la continuidad de sus negocios o la competitividad. La Estrategia apela reiteradamente a la colaboración público-privada para atender las obligaciones de la seguridad nacional, pero no recoge expresamente el derecho a participar -ser corresponsable-- en aquellas decisiones que afecten sus intereses económicos e industriales especialmente de las empresas que son sujetos principales de las obligaciones regulatorias[4]. Sí que se reconoce la necesidad de incrementar la colaboración con el sector privado en relación con la gestión de crisis, una cooperación que desde el sector privado se entiende de doble vía, porque las crisis también afectan a la imagen y continuidad de su negocio.

Algunas de las propuestas pendientes se pueden subsanar cuando se regule el Foro. Su creación (Línea de actuación, L.A. 3.9), da satisfacción a una exigencia recogida en la Ley de Seguridad Nacional, atiende una demanda reiterada del sector privado y representa un avance respecto a la Estrategia anterior. Su regulación queda pendiente, pero puede ayudar a construir una corresponsabilidad más equitativa, si las sinergias que se pretenden crear se orientan al desarrollo de las oportunidades económicas de la digitalización y no sólo, como hasta ahora, a desarrollar medidas de seguridad. Por eso, nuestras propuestas reivindicaban no sólo su creación sino, también, su participación en el nivel estratégico de las decisiones que afecten al sector. Un Foro marginal, sin presencia y capacidad de influencia en los centros donde se deciden las cuestiones que afecten al sector privado y a la sociedad, no tendría sentido en una política como la de ciberseguridad cuyo objetivo último es asegurar la prosperidad y el disfrute de la economía digital.

Los compromisos del sector público

Otra de las propuestas del sector privado, tenía que ver con la mayor asunción de compromisos por parte del sector público. Por un lado, se pedía que la Estrategia incluyera mecanismos de evaluación para verificar el cumplimiento de las medidas de seguridad acordadas para proteger los sistemas públicos y privados con el fin de asegurar que ambos sectores cumplen sus compromisos. En un sistema en las que el sector público establece obligaciones públicas y privadas, no parecía lógico que sólo se exigiera el cumplimiento de estas al sector privado, mientras que el sector público podría retrasar la ejecución de las obligaciones contempladas en los planes de acción o sectoriales por motivos políticos o presupuestarios. En la Estrategia, el Sistema se compromete a elaborar un informe anual de evaluación donde figurará el grado de ejecución y el cumplimiento de sus objetivos. Una autoevaluación es siempre mejor que

[4] No deja de resultar paradójico que se reconozca la necesidad de participación del sector privado en la regulación multilateral de la ciberseguridad y no se le reconozca esa misma necesidad en la regulación nacional, salvo que la regulación futura del Foro lo establezca.

ningún método de evaluación, como ocurría con la anterior Estrategia, y dará mucho juego y relevancia a la Comisión Mixta de Seguridad Nacional.

Las recomendaciones iban más allá de la exigencia al sector público y pedían reforzar la exigencia de cumplimiento de las obligaciones privadas, abarcando toda la cadena de suministro e implantando nuevas obligaciones como la de que cada empresa disponga de un CISO, un plan de riesgos, la obligación legal de presentar un informe a los consejos de administración de las sociedades que cotizan o a las presidencias de las agencias públicas. La Estrategia no ha entrado en la regulación obligatoria de estas materias, con los que se mantiene el margen de vulnerabilidad que se señala en las cadenas de suministro. Si que se ha comprometido a fomentar la normalización y la exigencia de requisitos en los productos y servicios de tecnologías de la información y de las comunicaciones, promoviendo la evaluación de la conformidad y la certificación. También se compromete a desarrollar mecanismos e indicadores agregados de riesgo adecuados a las condiciones de ciberseguridad, en lugar de vincularlo a las condiciones genéricas de riesgo como el nivel de alerta terrorista u otros como ocurría hasta ahora (L.A. 3.4 y 3.6), así como a crear mecanismos ágiles y seguros de denuncia para el sector privado como se le venía solicitando.

Finalmente, y ante el incremento imparable de los ciberataques, se le pedía al sector público que elevara su nivel de disuasión regulando la defensa activa y consolidando instrumentos de ciberdiplomacia y ciberdefensa en situaciones de particular gravedad. La Estrategia ha aceptado comprometer al sector público y al privado en la gestión de los riesgos de la cadena de suministro, especialmente en aquellas certificaciones críticas que afecten a la provisión de servicios esenciales, pero sólo propone recurrir a medidas de ciberdefensa activa para proteger ciudadanos y pymes (L.A. 3.5). De esta forma sigue pendiente la cuestión de si el sector público llevaría a cabo medidas de defensa activa en apoyo de las empresas e industrias principales o si las cogestionaría con estas. En todo caso, el reconocimiento del derecho a la defensa activa como se le pedía representa un avance en esa dirección.

La cuestión industrial

La cuestión industrial es una parte de la seguridad económica que sigue pendiente de la necesaria atención. La ciberseguridad, además de riesgos, también genera oportunidades para las empresas e industrias que se preparan para aprovechar el creciente mercado global de la ciberseguridad. La nueva Estrategia, a diferencia de la anterior, se muestra mucho más ambiciosa en este ámbito, aunque las posibilidades de que esa ambición se convierta en políticas industriales, de investigación y desarrollo, exceden a las capacidades propias del Sistema[5].

[5] El desarrollo de las tecnologías asociadas con la digitalización (ciberseguridad, inteligencia artificial, robótica, automatización, computación cuántica y otras) carece todavía de un marco industrial integrado. Para su necesidad, ver “La cuarta revolución industrial. Un enfoque de seguridad nacional”, DT 12/2018, Real Instituto Elcano, http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/dt12-2018-arteaga-cuarta-revolucion-industrial-enfoque-seguridad-nacional.

Por ejemplo, la Estrategia se muestra dispuesta a apoyar aquellas necesidades específicas que sustenten necesidades de interés nacional para fortalecer la autonomía digital, y la propiedad intelectual e industrial (L.A. 4.3), pero no identifica, como se le recomendaba desde el sector privado, aquellas tecnologías críticas para la ciberseguridad nacional que no deban depender de terceros ni se concreta la forma en la que se apoyarán esas necesidades. La identificación de las tecnologías críticas favorecería la protección de la compra pública por razones de seguridad nacional en el marco de la Unión Europea, y facilitaría la consolidación del sector tecnológico e industrial de la ciberseguridad.

También se solicitaba que el Estado fomentara, en su acción exterior, el desarrollo de asociaciones estratégicas bilaterales con empresas presas y estados líderes del sector para potenciar su base tecnológica e industrial y establecer acuerdos y alianzas estratégicas con los suministradores internacionales de referencia y confianza, de forma que permitieran desarrollar el tejido empresarial nacional y facilitar su acceso a la tecnología y mercados (partenariados) pero el Objetivo IV de la Estrategia no menciona ninguna línea de actuación económica en ese sentido.

A pesar de lo anterior, no se puede negar a la nueva Estrategia dedica mucha mayor atención a las cuestiones industriales que la anterior y que ha admitido bastantes de las propuestas que se le hacían desde el sector privado. Entre otras líneas de actuación que se propone desarrollar para impulsar la industria española de ciberseguridad figuran, las de compra pública innovadora (L.A. 4.1), medidas de apoyo a la innovación, a la inversión, a la internacionalización y a la transferencia tecnológica en especial en el caso de micropymes y pymes (L.A. 4.2), a la seguridad desde el diseño, (L.A. 4.3), identificar las necesidades de capacidades profesionales y educativas, impulsando la formación continua y promoviendo sistemas de acreditación y certificación profesional (L.A. 4.7). Todas estas líneas de acción están bien orientadas y coinciden con las recomendadas por el sector privado, pero carecen de garantías concretas de ejecución en términos de recursos, responsables y plazos, por lo que, nuevamente, la concreción de la forma en la que se llevarán a cabo se posterga para más adelante, cuando se formulen los planes de acción y sectoriales oportunos.

Conclusión

La revisión de la Estrategia de Ciberseguridad Nacional de 2013 se ha llevado a cabo de una forma rápida y solvente, lo que revela la madurez técnica del Sistema de Ciberseguridad Nacional. Bien es cierto que la Estrategia, como todas las estrategias técnicas, son más fáciles de elaborar cuanto menos se concretan en los detalles de su ejecución y menos actores intervienen en su elaboración.

La Estrategia contiene directrices transformacionales que apuntan en la buena dirección, pero no las acompaña de la identificación de los recursos, responsables y plazos que harían posible su desarrollo. Tampoco identifica los objetivos a lograr, por lo que no se puede medir -ni criticar- su grado de progreso hacia ellos. Desarrollada desde dentro del Sistema, la Estrategia sigue siendo de Ciberseguridad Nacional, aunque ahora se denomina Nacional de Ciberseguridad, porque en su elaboración no ha

participado el resto de los actores públicos y privados implicados, aunque se les haya a dado a conocer su texto ya escrito.

Corresponde ahora al futuro Gobierno concretar con prioridades, presupuestos y mandatos las directrices técnicas de la Estrategia. Desde el punto de vista del sector privado, la Estrategia codifica y abre la puerta a una mayor cooperación con el sector público, especialmente a través del Foro de Ciberseguridad Nacional. La responsabilidad para hacerlo no sólo depende del Gobierno y del Sistema, sino que comienza por el mismo sector privado, por su capacidad de articularse y organizarse para facilitar su interlocución e influencia con el sector público. Tras la Estrategia, y después de tanto solicitarlo, la “pelota” de la cooperación público-privada se encuentra ahora en el tejado del sector privado.