COMISIÓN
EUROPEA

Bruselas, 12.9.2018
SWD(2018) 404 final

DOCUMENTO DE TRABAJO DE LOS SERVICIOS DE LA COMISIÓN

RESUMEN DE LA EVALUACIÓN DE IMPACTO

que acompaña al documento

PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

por el que se establecen el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de Coordinación

{COM(2018) 630 final} - {SEC(2018) 396 final} - {SWD(2018) 403 final}

Ficha resumen

Evaluación de impacto sobre la Propuesta de creación de la Red de Centros de Competencia y el Centro Europeo de Investigación y Competencia en Ciberseguridad

A. Necesidad de actuar

¿Por qué? ¿Cuál es el problema que se afronta?

La UE sigue sin tener las capacidades tecnológicas e industriales suficientes para garantizar de forma autónoma la seguridad de su economía y sus infraestructuras básicas y convertirse en un líder mundial en el ámbito de la ciberseguridad. La presente iniciativa tiene por objeto contribuir a abordar los siguientes problemas y factores afines de la mencionada situación:

Problema n.º 1: Hay un grado insuficiente de coordinación y cooperación estratégicas y duraderas entre las industrias, las comunidades investigadoras del ámbito de la ciberseguridad y los Gobiernos para proteger la economía, la sociedad y la democracia con ayuda de soluciones europeas de ciberseguridad de vanguardia.

Problema n.º 2: Se invierte a escala reducida y hay un acceso limitado a conocimientos técnicos, capacidades e instalaciones relacionados con la ciberseguridad en toda Europa.

Problema n.º 3: Son pocos los resultados de la investigación y la innovación europeas en el ámbito de la ciberseguridad que se traducen en soluciones comercializables y se implantan de manera generalizada en los distintos sectores de la economía.

Hay una serie de factores subyacentes a estos problemas, como la falta de confianza entre los diferentes agentes del mercado de la ciberseguridad, las limitaciones inherentes de los mecanismos actuales de cooperación y puesta en común de fondos, la ausencia de un marco para la contratación conjunta de infraestructuras y productos/soluciones de ciberseguridad costosos, o el potencial no aprovechado de los mecanismos de mercado de impulso y atracción (*push-pull*).

¿Cuál es el objetivo que se espera alcanzar con esta iniciativa?

El objetivo de la iniciativa es conseguir que la UE conserve y desarrolle las capacidades fundamentales (tecnológicas e industriales) para garantizar de forma autónoma la seguridad de su economía digital, su sociedad y su democracia, y que los Estados miembros se beneficien de las soluciones de ciberseguridad y las capacidades de ciberdefensa más avanzadas. Asimismo, la iniciativa se propone aumentar la competitividad a escala mundial de las empresas de ciberseguridad de la UE y garantizar que las industrias europeas de cualquier sector tienen acceso a las capacidades y los recursos necesarios para hacer de la ciberseguridad su ventaja competitiva. A tal fin, es preciso crear mecanismos eficaces que propicien una cooperación estratégica y a largo plazo entre todos los agentes pertinentes (autoridades públicas, industrias, comunidad investigadora de los ámbitos civil y militar), poner en común los conocimientos y recursos necesarios para proporcionar capacidades e infraestructuras de vanguardia, promover una amplia implantación de los productos y soluciones europeos de ciberseguridad en los distintos sectores de la economía y en el sector público, apoyar a las empresas emergentes y las pymes del ámbito de la ciberseguridad, y ayudar a colmar las lagunas de capacidades en materia de ciberseguridad.

¿Cuál es el valor añadido de la actuación a nivel de la UE?

La iniciativa añadiría valor a los esfuerzos que ya se realizan en el ámbito nacional al contribuir a crear un ecosistema industrial y de investigación en ciberseguridad interconectado a escala europea. Asimismo, debería fomentar una mayor cooperación entre las distintas partes interesadas (también entre los sectores civil y militar de ciberseguridad) con el fin de utilizar de manera óptima los recursos y conocimientos especializados en ciberseguridad actuales que están dispersos por toda Europa. La iniciativa debería contribuir a que la UE y los Estados miembros adopten una perspectiva proactiva, a más largo plazo y estratégica respecto de la política industrial en materia de ciberseguridad que vaya más allá de la investigación y el desarrollo. Este planteamiento debería ayudar no solo a encontrar soluciones avanzadas a los problemas de ciberseguridad que se les plantean a los sectores público y privado, sino también a apoyar la aplicación efectiva de estas soluciones. También hará posible que las comunidades investigadora e industrial pertinentes y las autoridades públicas accedan a capacidades fundamentales, como instalaciones de ensayo y experimentación, que con frecuencia están fuera del alcance de los diferentes Estados miembros debido a unos recursos financieros y humanos insuficientes.

Asimismo, contribuirá a colmar el déficit de capacidades y a evitar la fuga de cerebros al posibilitar el acceso de los mejores talentos a grandes proyectos europeos y proponer por tanto interesantes desafíos profesionales. Todo lo anterior también se considera necesario para que Europa sea reconocida mundialmente como un líder en ciberseguridad.

B. Soluciones

¿Qué opciones legislativas y no legislativas se han estudiado? ¿Existe o no una opción preferida? ¿Por qué?

Se ha tenido en cuenta una serie de opciones políticas, tanto legislativas como no legislativas. A continuación se indican las opciones escogidas para una evaluación a fondo:

1. **Hipótesis de referencia** (opción de colaboración): supone la continuación del enfoque actual de creación de capacidades industriales y tecnológicas de ciberseguridad en la UE mediante el apoyo a la investigación y la innovación y los correspondientes mecanismos de colaboración en el marco del programa Horizonte Europa.
2. **Opción 1:** Red de competencias en ciberseguridad, junto con un Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad facultado para aplicar medidas de apoyo a las tecnologías industriales y en el ámbito de la investigación y la innovación.
3. **Opción 2:** Red de competencias en ciberseguridad, junto con un Centro Europeo de Investigación y Competencia en Ciberseguridad dedicado únicamente a actividades de investigación e innovación.

Entre las opciones descartadas en una fase inicial figuraban las siguientes: 1) no adoptar ninguna medida, 2) una red de los centros de competencia ya existentes únicamente, y 3) uso de una agencia existente (ENISA, REA o INEA).

En vista del compromiso general ya asumido por la Comisión en relación con la presente iniciativa, así como en vista del importante papel que deben desempeñar los Estados miembros, la principal distinción entre las dos opciones políticas analizadas en detalle radica en su alcance, como se refleja en su base jurídica: una entidad basada únicamente en el artículo 187 del TFUE (opción 2) limitaría la iniciativa al ámbito de la investigación y la innovación, y, en principio, requeriría una contribución financiera de agentes privados. Por otra parte, una entidad con una base jurídica doble, esto es, los artículos 187 y 173 del TFUE (opción 1), supondría un mandato más amplio que, entre otros aspectos, abarcaría también la implantación y el apoyo a la industria, y daría lugar a sinergias más sólidas con la ciberdefensa. Asimismo, implicaría un papel más destacado para los Estados miembros, desde el punto de vista tanto de su función en la gobernanza como de su función de compradores potenciales de tecnología de ciberseguridad.

El análisis mostró que la opción 1 es la más adecuada para alcanzar los objetivos de la iniciativa, al tiempo que ofrece la mayor repercusión económica, social y medioambiental y salvaguarda los intereses de la Unión. Entre los principales argumentos a favor de esta opción se encuentran la flexibilidad para permitir diferentes modelos de cooperación con la Comunidad y la Red de Centros de Competencia a fin de optimizar el uso de los conocimientos y recursos existentes; la capacidad para estructurar la cooperación de las partes interesadas, públicas y privadas, de todos los sectores pertinentes, incluido el de la defensa; y la capacidad para crear una auténtica política industrial de ciberseguridad al apoyar actividades relacionadas no solo con la investigación y el desarrollo, sino también con la implantación en el mercado. Por último, la opción 1 favorece igualmente que haya una mayor coherencia al servir como mecanismo de ejecución de la financiación relativa a la ciberseguridad procedente del programa Europa Digital y de Horizonte Europa, y permite reforzar las sinergias entre los aspectos civil y militar de la ciberseguridad en relación con el Fondo Europeo de Defensa.

¿Quién apoya cada opción?

De acuerdo con los resultados de los procesos de consulta y de recogida de pruebas, tanto la comunidad industrial como la comunidad investigadora demandan claramente un mecanismo que permita a la UE disponer de una política industrial coherente en materia de ciberseguridad que vaya más allá de las actividades de investigación e innovación si la idea es que Europa se convierta en un líder mundial en ciberseguridad. Asimismo, las partes interesadas han hecho hincapié en que las claves para el éxito son definir adecuadamente el papel del Centro en lo referente al apoyo a los esfuerzos de la Red y las comunidades pertinentes, así como la facilitación

de estos esfuerzos, y adoptar un enfoque inclusivo y colaborativo para la Red a fin de evitar que surjan nuevos «compartimentos estancos». En vista de que la ciberseguridad es un ámbito que evoluciona con rapidez, la estructura debe, además, ser flexible, de manera que se pueda adaptar fácilmente. A lo largo del proceso, los Estados miembros han recalcado la necesidad de incluir a todos los Estados miembros y sus centros de excelencia y competencia existentes, así como la necesidad de prestar especial atención a la complementariedad de las acciones. En lo que se refiere específicamente al Centro, los Estados miembros han destacado la importancia de su función de coordinación en apoyo a la Red. Por tanto, la Comisión, en la iniciativa que proponga, deberá hallar el equilibrio adecuado en las estructuras de gobernanza y ejecución y reflejar ese equilibrio en tales estructuras a fin de garantizar una coordinación europea eficaz, al mismo tiempo que se tiene en cuenta la evolución a escala nacional.

C. Repercusiones de la opción preferida

¿Cuáles son las ventajas de la opción preferida (si existe, o bien de las principales)?

La opción preferida permitirá a las autoridades públicas y las industrias de todos los Estados miembros prevenir y actuar ante las ciberamenazas de manera más eficaz ofreciendo y equipándose con productos y soluciones más seguros. Esto es especialmente importante de cara a la protección del acceso a los servicios básicos (por ejemplo, el transporte, la salud, la banca o los servicios financieros). Asimismo, tendría una repercusión positiva en la competitividad y las pymes de la UE, ya que supone el establecimiento de un mecanismo que permitiría crear capacidades industriales en materia de ciberseguridad en los Estados miembros y en la Unión, y lograr que la excelencia científica de Europa se traduzca efectivamente en soluciones comercializables que puedan implantarse en los distintos sectores de la economía. Esta opción hace posible la puesta en común de recursos para invertir en las capacidades necesarias en los Estados miembros y desarrollar activos europeos compartidos, al tiempo que se consiguen economías de escala. En consecuencia, es probable que las pymes, las industrias y los investigadores puedan acceder con mayor facilidad a tales infraestructuras, lo que estimulará la innovación y acortará los procesos de desarrollo. Por otra parte, esto reducirá los costes para algunas empresas de la demanda y las ayudará a convertir la ciberseguridad en su ventaja competitiva. La opción permite, además, aprovechar las oportunidades de mercado de las tecnologías de doble uso, ya que las comunidades civil y militar pueden colaborar para resolver desafíos comunes. También es probable que añada valor a los esfuerzos nacionales dirigidos a hacer frente al déficit de capacidades en materia de ciberseguridad. A escala de la UE, esta opción favorece la coherencia y las sinergias entre diferentes mecanismos de financiación.

Cabe también la posibilidad de generar repercusiones positivas indirectas para el medio ambiente mediante el desarrollo de soluciones específicas de ciberseguridad que ayuden a los sectores que pueden tener un gran impacto medioambiental (por ejemplo, las centrales nucleares) a evitar las consecuencias potencialmente devastadoras de los ataques de ciberseguridad a este tipo de infraestructuras.

¿Cuáles son los costes de la opción preferida (si existe, o bien de las principales)?

Los costes derivados de la opción preferida atañen principalmente a los costes de funcionamiento del Centro y los centros nacionales de coordinación. Los costes relativos a la ejecución de los diferentes programas de financiación (programa Europa Digital y programa Horizonte Europa) son objeto de evaluaciones de impacto independientes.

¿Cómo se verán afectadas las empresas, las pymes y las microempresas?

Las empresas europeas, tanto las de la demanda como las de la oferta de ciberseguridad, incluidas las pymes y las microempresas que ejercen sus actividades en el campo de la ciberseguridad, se encuentran entre los grupos de partes interesadas que se verán más afectados. El establecimiento del Centro de Competencia y la Red no conlleva la imposición de obligaciones normativas a las empresas; sin embargo, supondrá la creación de nuevas oportunidades desde el punto de vista de la reducción de los costes ligados al diseño de nuevos productos y hará que sea más fácil para las empresas acceder a la comunidad de inversores y captar la financiación necesaria para el desarrollo de soluciones comercializables. En el caso de las pymes y las microempresas, el hecho de poder acceder a instalaciones de ensayo y experimentación financiadas con fondos públicos reviste aún más importancia, ya que carecen de recursos para adquirir la infraestructura necesaria o para viajar fuera de su mercado (y a menudo fuera de la UE) en busca de dicha infraestructura. Se espera igualmente que la presente iniciativa abra nuevos mercados para las pymes y las microempresas europeas activas en el ámbito de la ciberseguridad. Además, el mecanismo elegido garantizará la coordinación entre el ámbito investigador y la

industria, y, en consecuencia, orientará los esfuerzos de investigación hacia las necesidades concretas de la industria. La provisión de conocimientos especializados e instrumentos punteros en materia de ciberseguridad ayudará de forma indirecta a los agentes económicos a cumplir la Directiva SRI.

¿Habrá repercusiones significativas en los presupuestos y las administraciones nacionales?

La iniciativa hará posible que los Estados miembros coordinen las inversiones en la infraestructura de ciberseguridad necesaria a escala nacional y europea. Asimismo, el mecanismo permitirá poner en común recursos destinados a instrumentos e infraestructuras que de otro modo serían más costosos o no serían asequibles para los Estados miembros. Por otra parte, se espera que este enfoque favorezca las economías de escala y la racionalización. La contribución financiera de los Estados miembros al Centro de Competencia y las acciones correspondientes ha de ser proporcional a la contribución de la Unión.

¿Habrá otras repercusiones significativas?

Sí, la iniciativa tendrá una clara repercusión positiva, dado que es probable que conlleve un aumento significativo de las capacidades de los Estados miembros para garantizar de forma autónoma la seguridad de sus economías, incluida la protección de sus sectores básicos, así como un aumento de la competitividad de las empresas europeas de ciberseguridad y las industrias de diferentes sectores, que estarán en condiciones de garantizar debidamente la seguridad de sus activos y diseñar productos innovadores y seguros, al mismo tiempo que se reducen los costes de la I+D en relación con la seguridad. En última instancia, se espera que esto ayude a la UE a convertirse en un líder en cuanto a tecnologías digitales y de ciberseguridad de próxima generación.

D. Seguimiento

¿Cuándo se revisará la política?

El instrumento legislativo contendrá una cláusula explícita de seguimiento de los indicadores clave de resultados (ICR), así como una cláusula de evaluación y revisión, en virtud de las que la Comisión Europea llevará a cabo una evaluación intermedia para medir la repercusión del instrumento y su valor añadido. Posteriormente, la Comisión Europea informará de ello al Parlamento Europeo y al Consejo. A raíz de la evaluación, la Comisión podrá proponer una revisión y la ampliación del mandato del Centro de Competencia y la Red.