



Bruselas, 13.9.2017
SWD(2017) 501 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

relativo a ENISA, la «Agencia de Ciberseguridad de la UE», y por el que se deroga el Reglamento (UE) n.º 526/2013, y relativo a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación («Reglamento de Ciberseguridad»)

{ COM(2017) 477 final }

{ SWD(2017) 500 final }

{ SWD(2017) 502 final }

A. NECESIDAD DE ACTUAR

¿Cuál es el problema y por qué lo es?

Las tecnologías digitales e internet constituyen la espina dorsal de la economía y de la sociedad de la UE. Sectores económicos vitales, como el transporte, la energía, la salud o las finanzas, se han vuelto cada vez más dependientes de las redes y los sistemas de información para llevar a cabo sus actividades principales. La internet de las cosas conecta objetos y personas a través de las redes de comunicación. Esta nueva realidad crea oportunidades sin precedentes, pero también puntos vulnerables. Y ciertamente el número de ciberincidentes se dispara. Su complejidad, su frecuencia y la «superficie» de su impacto (desde el acceso a los servicios esenciales a los procesos democráticos) no van a dejar de aumentar.

En este contexto, se han detectado los siguientes problemas interrelacionados:

- fragmentación de las políticas y enfoques en materia de ciberseguridad en los distintos Estados miembros;
- dispersión de los recursos y enfoques en materia de ciberseguridad en las instituciones, órganos y organismos de la UE;
- conocimiento insuficiente de las ciberamenazas por parte de ciudadanos y empresas e información insuficiente sobre las propiedades de seguridad de los productos y servicios de TIC que adquieren, junto con la creciente aparición de múltiples regímenes de certificación nacionales y sectoriales.

Estos problemas repercuten en la ciberresiliencia global de la UE, así como en el buen funcionamiento del mercado interior.

¿Qué se pretende conseguir?

Los objetivos políticos específicos de la presente iniciativa son los siguientes:

1. Aumentar las capacidades y la preparación de los Estados miembros y de las empresas, en particular en lo referente a las infraestructuras críticas.
2. Mejorar la cooperación y la coordinación entre los Estados miembros y las instituciones, órganos y organismos de la UE.
3. Aumentar las capacidades a nivel de la UE para complementar la acción de los Estados miembros, en particular en caso de ciber crisis transfronteriza.
4. Aumentar la sensibilización de los ciudadanos y las empresas sobre las cuestiones relacionadas con la ciberseguridad.
5. Aumentar en general la transparencia de la garantía de ciberseguridad de los productos y servicios de TIC, a fin de reforzar la confianza en el mercado único digital y en la innovación digital.
6. Evitar la fragmentación, en los distintos Estados miembros y sectores, de los sistemas de certificación en la UE y los requisitos de seguridad y criterios de evaluación conexos.

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

Dado que la digitalización y la interconexión de la economía y la sociedad tienen un alcance global, la dimensión de los problemas va mucho más allá del territorio de un solo Estado miembro. Ello exige, por tanto, una intervención a nivel de la Unión. En el contexto actual, y teniendo en cuenta las hipótesis sobre el futuro, parece que las acciones individuales de los Estados miembros y un enfoque fragmentado en materia de ciberseguridad, vista sobre todo su importante dimensión transfronteriza, no pueden incrementar la ciberresiliencia colectiva de la Unión.

B. SOLUCIONES

¿Cuáles son las distintas opciones posibles para alcanzar los objetivos? ¿Existe o no una opción preferida?

La presente evaluación de impacto examina una serie de opciones políticas, que abarcan la revisión de la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA) y la certificación de seguridad de las TIC.

Revisión de ENISA

Opción 0 - Hipótesis de referencia - Esta opción consiste en el mantenimiento del *statu quo*. Se prorrogaría el mandato de ENISA y los objetivos y cometidos de la Agencia se mantendrían básicamente sin cambios, teniendo al mismo tiempo en cuenta las tareas encomendadas a ENISA por la legislación posterior de la UE (por ejemplo, la Directiva SRI).

Opción 1 - Expiración del mandato de ENISA (fin de ENISA). Esta opción pondría fin a ENISA al concluir su mandato (junio de 2020) y supondría posiblemente una redistribución de competencias/actividades a nivel de la UE o nacional.

Opción 2 - Reforma de ENISA. Esta opción partiría del actual mandato de ENISA, con vistas a adoptar modificaciones selectivas que tengan en cuenta la evolución del panorama de la ciberseguridad. La Agencia obtendría un mandato permanente, basado en los siguientes pilares: apoyo a la elaboración y ejecución de las políticas de la UE; creación de capacidades; conocimientos e información; tareas relacionadas con el mercado; investigación e innovación; y cooperación operativa y gestión de crisis.

Opción 3 - Una agencia de ciberseguridad de la UE con plena capacidad operativa. Esta opción supone reformar ENISA reuniendo tres funciones principales: 1. Una función política/consultiva; 2. Un centro de información y conocimientos, y 3. Un equipo de respuesta a emergencias informáticas (CERT). En gran medida, esta opción implicaría el mismo cambio en el alcance del mandato que la opción 2. Sin embargo, podrían incluirse tareas adicionales en el ámbito de la gestión de crisis y de respuesta a incidentes, con el fin de que la Agencia pudiera cubrir todo el ciclo de vida de la ciberseguridad y abordar la prevención, detección y respuesta a ciberincidentes.

Certificación

Opción 0 - Hipótesis de referencia - no hacer nada. Con arreglo a esta opción, la Comisión mantendría el *statu quo* y no emprender ninguna acción legislativa ni política.

Opción 1 - **Medidas no legislativas (Derecho indicativo)**. Con arreglo a esta opción, la Comisión utilizaría instrumentos políticos flexibles (por ejemplo, comunicaciones interpretativas, apoyo a las iniciativas de autorregulación y las actividades de normalización a escala de la UE) a fin de mejorar la transparencia y reducir la fragmentación.

Opción 2 - **Un acto legislativo de la UE para hacer extensivo a todos los Estados miembros el acuerdo SOG-IS**. Con arreglo a esta opción, la Comisión propondría un acto legislativo para incluir jurídicamente a todos los Estados miembros.

Opción 3 - **Un marco general de certificación de la ciberseguridad de las TIC en la UE**. Esta opción implica el establecimiento de un marco europeo de certificación de la seguridad de las TIC (incluido un grupo de expertos compuesto por autoridades nacionales), apoyándose en la medida de lo posible en los regímenes de certificación de la seguridad de las TIC ya existentes. En esencia, el marco permitiría el establecimiento de regímenes de certificación de la UE aceptados en todos los Estados miembros.

La opción preferida es una combinación de la opción 2 para ENISA y de la opción 3 para la certificación.

¿Cuáles son las distintas partes interesadas? ¿Quién apoya cada opción?

La gran mayoría de las partes interesadas de todas las categorías (Estados miembros, industria, instituciones de la UE, comunidad investigadora) que participaron en las consultas parece a favor de la opción preferida, ya que supone reforzar ENISA y crear un marco europeo de certificación de la seguridad de las TIC.

En particular, existe consenso sobre la necesidad de disponer (como mínimo) de una agencia de la UE que funcione correctamente con un mandato permanente y cuente con los recursos y el mandato adecuados para hacer frente a los retos actuales y futuros en materia de ciberseguridad. También existe un amplio consenso entre las partes interesadas sobre la creación de un marco europeo voluntario y modulable.

En la industria, esta solución para la certificación está respaldada por las empresas que ya están sujetas a requisitos de certificación, a las que favorecería un mecanismo a escala de la UE basado en el reconocimiento mutuo de certificados. También la apoyan las pymes, que son las que más sufren cuando tienen que embarcarse en diferentes procesos de certificación en distintos Estados miembros o sufrirían si tuvieran que hacerlo. Algunos Estados miembros, en particular los que disponen de menos recursos, y algunos representantes de la industria y de las instituciones de la UE también manifestaron una opinión positiva por lo que se refiere a la opción 3 para ENISA.

C. REPERCUSIONES DE LA OPCIÓN PREFERIDA

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

En el marco de la opción preferida, la UE dispondría de una agencia centrada en prestar apoyo a los Estados miembros, las instituciones de la UE y de las empresas en las áreas donde pudiera aportar más valor añadido. Se trataría de: apoyo a la aplicación de la Directiva SRI; elaboración y ejecución de políticas; información, conocimientos y sensibilización; investigación; cooperación operativa y gestión de crisis; mercado. En particular, ENISA

apoyaría la política de la UE en el ámbito de la certificación de la seguridad de las TIC, velando por el mantenimiento administrativo y la gestión técnica de un marco europeo de certificación de seguridad de las TIC. Dicho marco establecería de manera efectiva un conjunto de normas sobre la gobernanza de la certificación de la seguridad de las TIC en la UE, que promovería un régimen de reconocimiento mutuo de los certificados expedidos en todos los Estados miembros. La solución que combina estas opciones se considera la más eficaz para que la UE alcance los objetivos señalados de: aumentar las capacidades de ciberseguridad; preparación; cooperación; sensibilización; transparencia; y evitación de la fragmentación del mercado. Esta opción es también la más coherente con las prioridades políticas, tal como se consagran en la Estrategia de Ciberseguridad y medidas conexas (por ejemplo, la Directiva SRI), y en la Estrategia para el Mercado Único Digital. Además, esta opción permitiría alcanzar los objetivos mediante un empleo razonable de los recursos.

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

Pese a la adquisición de nuevas funciones, la «ENISA reformada» seguirá siendo una organización ágil. La contribución financiera del presupuesto de la UE necesaria sería superior a la actual, pero seguiría bastante por debajo de otras agencias que también operan en áreas críticas.

La creación de un marco europeo de certificación de la seguridad de las TIC no implicaría costes adicionales iniciales para la industria (incluidas las pymes). Supondría al contrario un ahorro considerable para las empresas que ya certifican sus productos o están dispuestas a efectuar la certificación de la seguridad, con repercusiones positivas para su competitividad en el mundo. Por otro lado, implicaría a algunos compromisos presupuestarios para garantizar el mantenimiento del marco, que deberían proceder en su mayor parte del modelo de la «ENISA reformada», en lo que se refiere a las tareas técnicas y de secretaría.

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

No. Los costes asociados al refuerzo de ENISA serían principalmente con cargo al presupuesto de la UE, aunque los Estados miembros aún podrían aportar contribuciones financieras voluntarias a la Agencia. En cuanto a la certificación, las principales repercusiones sobre los presupuestos y la administración nacionales derivarían de la creación de una autoridad de certificación, en su caso.

¿Habría otras repercusiones significativas?

No

Proporcionalidad

La opción preferida incluye medidas equilibradas, todas ellas consideradas necesarias para alcanzar los objetivos previstos, sin por ello imponer una carga excesiva a los interesados. En vista de ello, se considera que la presente iniciativa se ajusta al principio de proporcionalidad.

D. SEGUIMIENTO

¿Cuándo se revisará la política?

Se propone ahora que la primera evaluación tenga lugar cinco años después de la entrada en vigor del instrumento jurídico. Posteriormente, la Comisión informará al Parlamento Europeo y al Consejo sobre su evaluación, adjuntando cuando proceda una propuesta para su revisión. Se llevarán a cabo evaluaciones posteriores cada cinco años.