Consejo de la Unión Europea

Bruselas, 18 de diciembre de 2020
(OR. en)

14150/20
ADD 3

Expediente interinstitucional: 2020/0359 (COD)

CYBER 281
JAI 1119
DATAPROTECT 155
TELECOM 270
MI 581
CSC 368
CSCI 97

NOTA DE TRANSMISIÓN

De:	Por la secretaria general de la Comisión Europea, D.ª Martine DEPREZ, directora
Fecha de recepción:	16 de diciembre de 2020
A:	D. Jeppe TRANHOLM-MIKKELSEN, secretario general del Consejo de la Unión Europea
N.° doc. Ción.:	SWD(2020) 344 final
Asunto:	DOCUMENTO DE TRABAJO DE LOS SERVICIOS DE LA COMISIÓN RESUMEN DEL INFORME DE LA EVALUACIÓN DE IMPACTO que acompaña al documento Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad y por la que se deroga la Directiva (UE) 2016/1148

Adjunto se remite a las Delegaciones el documento – SWD(2020) 344 final.

Adj.: SWD(2020) 344 final

COMISIÓN
EUROPEA

Bruselas, 16.12.2020
SWD(2020) 344 final

DOCUMENTO DE TRABAJO DE LOS SERVICIOS DE LA COMISIÓN

RESUMEN DEL INFORME DE LA EVALUACIÓN DE IMPACTO

que acompaña al documento

Propuesta de Directiva del Parlamento Europeo y del Consejo

relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad y por la que se deroga la Directiva (UE) 2016/1148

{COM(2020) 823 final} - {SEC(2020) 430 final} - {SWD(2020) 345 final}

Ficha resumen

Evaluación de impacto de la *revisión de la Directiva (UE) 2016/1148, 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 (en lo sucesivo, «la Directiva SRI»)*

A. Necesidad de actuar

¿Cuál es el problema y por qué es un problema a escala de la UE?

A pesar de que los logros conseguidos con la Directiva SRI han sido notables y con ella se sentaron las bases de un cambio de mentalidad significativo y la estrategia institucional y reglamentaria que muchos Estados miembros han aplicado a la ciberseguridad, también ha demostrado sus limitaciones con el tiempo. La transformación digital de la sociedad (agudizada por la crisis de la COVID-19) ha ampliado el panorama de amenazas e introduce nuevos desafíos, lo que exige respuestas adaptadas e innovadoras. El número de ciberataques continúa aumentando y los ataques son cada vez más sofisticados y proceden de un amplio abanico de fuentes de dentro y fuera de la UE.

A partir de la evaluación del funcionamiento de la Directiva SRI, en la evaluación de impacto se determinaron los siguientes problemas: el bajo nivel de ciberresiliencia de las empresas que operan en la UE; la incoherencia en términos de resiliencia entre Estados miembros y sectores, y el escaso nivel de conciencia situacional conjunta y la ausencia de una respuesta conjunta en caso de crisis. Por ejemplo, como resultado de algunos de estos problemas y factores impulsores, se dan situaciones en que hospitales importantes de un Estado miembro no están incluidos en el ámbito de aplicación de la Directiva SRI y, por ende, no están obligados a aplicar las correspondientes medidas de seguridad, mientras que en otro Estado miembro prácticamente todos los hospitales del país están cubiertos por los requisitos de seguridad de la Directiva.

¿Qué se pretende conseguir?

Con la revisión de la Directiva SRI se prevén tres objetivos generales:

1. **Incrementar el nivel de ciberresiliencia de un conjunto exhaustivo de empresas que operan en la Unión Europea en todos los sectores pertinentes,** mediante la implantación de normas que garanticen que todas las entidades públicas y privadas del mercado interior que desempeñen funciones importantes para la economía y la sociedad en su conjunto estén obligadas a adoptar medidas de ciberseguridad adecuadas.
2. **Reducir las incoherencias en términos de resiliencia en todo el mercado interior en los sectores que ya están cubiertos por la Directiva,** mediante una mayor armonización de 1) el ámbito de aplicación *de facto*, 2) los requisitos de seguridad y notificación de incidentes, 3) las disposiciones que rigen la supervisión y ejecución nacionales, y 4) las capacidades de las autoridades competentes en los Estados miembros.
3. **Mejorar el nivel de conciencia situacional conjunta y la capacidad colectiva de preparación y respuesta,** mediante la adopción de medidas destinadas a incrementar el nivel de confianza entre las autoridades competentes, el intercambio de más información y la fijación de normas y procedimientos en caso de que se produzca un incidente o crisis a gran escala.

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

La resiliencia en términos de ciberseguridad en toda la Unión no puede ser eficaz si se aplican distintos enfoques de carácter nacional o regional. La Directiva SRI solucionó esta deficiencia al establecer un

marco para la seguridad de las redes y los sistemas de información a escala nacional y de la Unión. No obstante, su transposición y aplicación también puso de manifiesto los defectos inherentes de determinadas disposiciones o enfoques, como por ejemplo la ambigua delimitación del ámbito de aplicación de la Directiva SRI. Por otro lado, desde el estallido de la crisis de la COVID-19, la dependencia de la economía europea de las redes y sistemas de información ha aumentado hasta niveles sin precedentes, y los sectores y servicios están cada vez más interconectados. Por consiguiente, la primera revisión periódica de la Directiva SRI brindó la oportunidad de reforzar la actuación de la UE. Los siguientes motivos justifican que la intervención de la UE trascienda las medidas actuales de la Directiva SRI: i) la naturaleza transfronteriza del problema; ii) el potencial de que la intervención de la UE mejore unas políticas nacionales efectivas y las facilite; y iii) la contribución de unas acciones políticas de SRI concertadas y colaborativas a la protección efectiva de los datos y la privacidad.

B. Soluciones

¿Cuáles son las distintas opciones posibles para alcanzar los objetivos? ¿Existe o no una opción preferida? De no ser así, ¿por qué no?

En la evaluación de impacto se analizaron cuatro opciones: 0) mantenimiento del *statu quo*; 1) medidas no legislativas para armonizar la transposición; 2) cambios limitados en la Directiva SRI en aras de una armonización mayor; 3) cambios sistémicos y estructurales en la Directiva SRI. La opción 1 se descartó en una fase temprana, ya que apenas se diferencia del *statu quo*. La evaluación de impacto determina que la **opción preferida** es la tercera, es decir, introducir **cambios sistémicos y estructurales en el marco de la SRI**, ya que contemplaría un cambio de enfoque más profundo destinado a abarcar un segmento más amplio de las economías de toda la Unión, aunque con una supervisión más centrada proporcionalmente en las empresas clave y de grandes dimensiones, al tiempo que se delimita el ámbito de aplicación. Asimismo, racionalizaría y armonizaría en mayor medida las obligaciones de seguridad impuestas a las empresas, crearía una configuración más efectiva para los aspectos operativos, establecería unos cimientos claros para reforzar las responsabilidades compartidas y la rendición de cuentas de los actores pertinentes, e incentivaría el intercambio de información.

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

La mayoría de las autoridades competentes y las empresas se mostraron a favor de revisar la Directiva SRI. A través de varias consultas, indicaron que una Directiva SRI revisada debía abarcar (sub)sectores adicionales y armonizar o racionalizar aún más las medidas de seguridad y las obligaciones de notificación. Por otro lado, las partes interesadas respaldaron nuevos conceptos o medidas relacionadas con la política que solo forman parte de la opción preferida (p. ej., políticas en materia de seguridad para la cadena de suministro, institucionalización de un marco operativo de la UE para la gestión de crisis).

C. Repercusiones de la opción preferida

¿Qué beneficios aporta la opción preferida (de haberla; si no, las principales)?

La opción preferida aportaría beneficios importantes: las estimaciones realizadas a partir de una modelización económica desarrollada por un estudio de apoyo para la revisión de la Directiva SRI indican que la opción preferida podría generar una reducción del coste de los incidentes de ciberseguridad de 11 300 millones EUR.

El ámbito de aplicación sectorial del marco SRI se ampliaría considerablemente, pero además de los beneficios mencionados, la carga que los requisitos SRI podrían crear, en particular desde el punto de vista de la supervisión, también se equilibraría tanto para las nuevas entidades cubiertas como para las

autoridades competentes. Ello se debe a que el nuevo marco SRI establecería un enfoque en dos niveles, centrado en las entidades grandes y clave y con un régimen de supervisión diferenciado que permite aplicar únicamente supervisión *a posteriori* (es decir, reactiva y sin la obligación general de documentar sistemáticamente el cumplimiento) para un gran número de ellas, en particular las que se consideran «importantes», pero no «esenciales».

En general, la opción preferida produciría compensaciones y sinergias eficientes, y de todas las opciones analizadas es la que tiene un mejor potencial para garantizar un nivel reforzado y coherente de ciberresiliencia de las entidades clave de toda la Unión que, en última instancia, se traduciría en un ahorro de costes tanto para las empresas como para la sociedad.

¿Cuáles son los costes de la opción preferida (de haberla; si no, de las principales)?

La opción preferida conllevaría determinados costes de conformidad y de ejecución para las autoridades competentes de los Estados miembros (se ha estimado un incremento general de entre el 20 y el 30 % aproximadamente). No obstante, el nuevo marco también entrañaría beneficios sustanciales gracias a una mejora de la visión general de las empresas clave y la interacción con ellas, el refuerzo de la cooperación operativa transfronteriza, así como mecanismos de asistencia mutua y revisión interpares. Con todo ello se produciría un aumento general de las capacidades de ciberseguridad en todos los Estados miembros.

Por lo que respecta a las empresas que estuviesen incluidas en el ámbito de aplicación del marco SRI, se calcula que tendrían que incrementar su gasto actual en seguridad informática en un 22 % como máximo durante los primeros años posteriores a la introducción del nuevo marco SRI (un 12 % en el caso de las empresas que ya están incluidas en el ámbito de aplicación de la Directiva SRI vigente). Aun así, este incremento medio del gasto en seguridad de las TIC produciría un beneficio proporcional a dichas inversiones, en particular como consecuencia de la reducción considerable del coste de los incidentes de ciberseguridad (que según las estimaciones ascienden a 11 300 millones EUR a lo largo de diez años).

¿Cuáles son las repercusiones en las pymes y la competitividad?

Las microempresas y las pequeñas empresas estarían excluidas del ámbito de aplicación del marco SRI en la opción preferida. En lo tocante a las empresas medianas, cabe esperar que se produjese un aumento del nivel de gasto en seguridad de las TIC durante los primeros años posteriores a la introducción del nuevo marco SRI. Al mismo tiempo, el endurecimiento de los requisitos de seguridad aplicables a estas entidades también incentivaría sus capacidades de ciberseguridad y ayudaría a mejorar su gestión de los riesgos relacionados con las TIC.

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

Habría repercusiones en los presupuestos y las administraciones nacionales: cabe prever un aumento aproximado de entre el 20 y el 30 % de los recursos a corto y medio plazo.

¿Habrá otras repercusiones significativas?

No se contempla ninguna otra repercusión negativa significativa. Se espera que la opción preferida promueva unas capacidades de ciberseguridad más sólidas y, por tanto, tendría un efecto de mitigación más sustancial en el número y la gravedad de los incidentes, incluidas las violaciones de la seguridad de los datos. Asimismo, es probable que tenga una repercusión positiva al garantizar unas condiciones de competencia equitativas en todos los Estados miembros para todas las entidades incluidas en el ámbito de aplicación del marco SRI y reduzca las asimetrías en el ámbito de la información sobre ciberseguridad.

¿Proporcionalidad?

La opción preferida no rebasa los límites estrictamente necesarios para lograr los objetivos específicos de manera satisfactoria. La armonización y racionalización previstas de las medidas de seguridad y las obligaciones de notificación atienden a las peticiones de los Estados miembros y de las empresas de mejorar el marco vigente.
D. Seguimiento
¿Cuándo se revisará la política?
La primera revisión se llevaría a cabo cincuenta y cuatro meses después de la entrada en vigor del instrumento jurídico. La Comisión presentaría un informe sobre su revisión al Parlamento Europeo y al Consejo. La revisión se prepararía con el apoyo de la ENISA y el Grupo de Cooperación..