Consejo de la Unión Europea

Bruselas, 24 de septiembre de 2020
(OR. en)

11052/20
ADD 2

Expediente interinstitucional: 2020/0268 (COD)

EF 229
ECOFIN 847
TELECOM 160
CYBER 169
IA 62
CODEC 872

NOTA DE TRANSMISIÓN

De:	secretaria general de la Comisión Europea, firmado por D. Jordi AYET PUIGARNAU, director
Fecha de recepción:	24 de septiembre de 2020
A:	D. Jeppe TRANHOLM-MIKKELSEN, secretario general del Consejo de la Unión Europea
N.° doc. Ción.:	SWD(2020) 204 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 por la que se modifican las Directivas 2006/43/CE, 2009/65/CE, 2009/138/UE, 2011/61/UE, 2013/36/UE, 2014/65/UE, (UE) 2015/2366 y (UE) 2016/2341

Adjunto se remite a las Delegaciones el documento – SWD(2020) 204 final.

Adj.: SWD(2020) 204 final

COMISIÓN
EUROPEA

Bruselas, 24.9.2020
SWD(2020) 204 final

This document corrects document SWD(2020) 204 final of 24.09.2020
Two references in the title of the cover page have been corrected.
Concerns the EN version only.
The text shall read as follows:

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

por la que se modifican las Directivas 2006/43/CE, 2009/65/CE, 2009/138/UE, 2011/61/UE, 2013/36/UE, 2014/65/UE, (UE) 2015/2366 y (UE) 2016/2341

{COM(2020) 596 final} - {SEC(2020) 309 final} - {SWD(2020) 203 final}

Ficha resumen

Evaluación de impacto de la propuesta de Reglamento sobre la resiliencia operativa digital en el sector financiero

A. Necesidad de actuar

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

El sector financiero hace un extenso uso de las tecnologías de la información y la comunicación (TIC). Es probable que la actual pandemia de COVID-19 fomente aún más esa tendencia, dadas las ventajas de garantizar un acceso remoto permanente a los servicios financieros. No obstante, la dependencia de las tecnologías digitales plantea algunos problemas; las empresas deben ser capaces de resistir ante una posible disfunción de las TIC, de modo que puedan solventarse los incidentes y amenazas digitales y mantenerse los servicios. En un sector financiero muy interconectado que presta servicios transfronterizos cruciales de los que depende la economía real, las vulnerabilidades derivadas de la dependencia de las TIC, si bien afectan a todos los sectores económicos, son especialmente pronunciadas debido: 1) al uso amplio y profundo de las TIC, y 2) a la posibilidad de que los efectos de un incidente operativo en una empresa financiera o subsector financiero se propaguen rápidamente a otras empresas o partes del sector financiero y, en última instancia, al resto de la economía.

Pese a lo avanzado del proceso de integración del sector financiero, ya sea desde la óptica del mercado o de la normativa, y a su capacidad para funcionar sobre la base de un único conjunto de normas armonizadas —el código normativo único de la UE—, la respuesta de la UE a las crecientes necesidades de resiliencia operativa, tanto en el plano horizontal como en el sectorial:

- bien ha consistido en una armonización mínima, dejando así margen para la interpretación nacional y, por ende, para la fragmentación del mercado único,
- bien ha sido demasiado general y de aplicación limitada, solventando en diverso grado el riesgo operativo global y regulando parcialmente algunos componentes de la *resiliencia* operativa digital (por ejemplo, la gestión de riesgos de las TIC, la notificación de incidentes y el riesgo de las TIC derivado de terceros), pero ignorando otros componentes (pruebas).

Hasta ahora, la intervención de la UE no ha abordado el riesgo operativo de manera adecuada a la necesidad de las empresas financieras de resistir frente a las vulnerabilidades de las TIC, responder a ellas y recuperarse en el supuesto de que se materialicen, ni tampoco proporciona a los supervisores financieros las herramientas necesarias para cumplir su cometido de contener la inestabilidad financiera derivada de dichas vulnerabilidades de las TIC.

Las lagunas e incoherencias actuales han dado lugar a una proliferación de iniciativas nacionales (por ejemplo, sobre pruebas) y planteamientos de supervisión (por ejemplo, en relación con la dependencia de terceros en el ámbito de las TIC) sin ninguna coordinación, que se traduce en solapamientos, requisitos duplicados y elevados costes administrativos y de cumplimiento para las empresas financieras transfronterizas, o en la persistencia de riesgos relacionados con las TIC que no se detectan ni se subsanan. En términos generales, la estabilidad y la integridad del sector financiero no están garantizadas, y el mercado único de servicios financieros sigue fragmentado, lo que debilita la protección de los consumidores y los inversores.

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

El objetivo general es reforzar la resiliencia operativa digital del sector financiero de la UE, racionalizando y modernizando la legislación financiera vigente de la UE e introduciendo nuevos requisitos para colmar las lagunas existentes, con el propósito de mejorar:

- la gestión de los riesgos de las TIC por parte de las empresas financieras,
- el conocimiento de las amenazas e incidentes que tienen los supervisores,
- las pruebas a las que las empresas financieras someten sus sistemas de TIC, y
- la supervisión de los riesgos derivados de la dependencia de las empresas financieras de proveedores terceros de TIC.

Más concretamente, la propuesta crearía unos mecanismos de notificación de incidentes más coherentes y sistemáticos, reduciendo así las cargas administrativas para las entidades financieras y reforzando la eficiencia de la supervisión.

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

El mercado único de servicios financieros de la UE se rige por un amplio conjunto de normas establecidas a nivel de la UE que permiten a las empresas financieras autorizadas en un Estado miembro prestar servicios en todo el mercado único gracias a un pasaporte de la UE. Así pues, el establecimiento de normas a nivel nacional no sería una forma eficaz de reforzar la resiliencia operativa de las empresas financieras que hacen uso del pasaporte de la UE. Por otra parte, a raíz de la crisis financiera, el código normativo único de la UE contiene

normas muy detalladas y prescriptivas que contemplan riesgos más «tradicionales», como los riesgos de crédito, de mercado, de contraparte y de liquidez. Las actuales disposiciones sobre el riesgo operativo son, por ahora, de carácter general. El refuerzo de la resiliencia operativa digital requiere que se reajusten las disposiciones sobre riesgos operativos ya definidas a nivel de la UE y que, por tanto, solo pueden modernizarse y complementarse a nivel de la UE.

B. Soluciones

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

La evaluación de impacto considera tres opciones, además de un escenario de referencia consistente en no tomar ninguna medida en lo que respecta a la legislación de la UE en materia de servicios financieros. En concreto:

- **«No intervenir»**: las normas sobre resiliencia operativa seguirían estando determinadas por el actual conjunto divergente formado por las disposiciones sobre servicios financieros de la UE —y en parte por la Directiva SRI—, así como por los regímenes nacionales actuales o futuros.
- **Opción 1, reforzar los colchones de capital**: se introduciría un colchón de capital adicional para aumentar la capacidad de las empresas financieras de absorber las pérdidas que podrían derivarse de una insuficiente resiliencia operativa.
- **Opción 2, texto normativo sobre resiliencia operativa digital en el ámbito de los servicios financieros**: se instituiría así un marco global a escala de la UE que estableciera normas sobre la resiliencia operativa digital de todas las entidades financieras reguladas, y que
    - regulara de forma más exhaustiva los riesgos de las TIC,
    - permitiera el acceso de los supervisores financieros a la información sobre incidentes relacionados con las TIC,
    - garantizara que las entidades financieras evalúen la eficacia de sus medidas preventivas y de resiliencia e identifiquen las vulnerabilidades de las TIC,
    - reforzara las normas sobre externalización que rigen la supervisión indirecta de los proveedores terceros de TIC,
    - posibilitara una supervisión directa de las actividades de los proveedores terceros de TIC cuando presten servicios a empresas financieras, e
    - incentivara, además, el intercambio de información sobre amenazas en el sector financiero.
- **Opción 3, texto normativo sobre resiliencia combinado con la supervisión centralizada de los proveedores terceros esenciales**: además de la adopción de un texto normativo sobre resiliencia operativa (opción 2), se crearía una nueva autoridad para supervisar a los proveedores terceros de servicios de TIC esenciales para las empresas financieras. Ello permitiría delimitar también más claramente el sector financiero, distinguiéndolo del ámbito de aplicación de la Directiva SRI.

La opción 2 es la preferida. En comparación con las demás opciones, es la que permite alcanzar la mayoría de los objetivos de la iniciativa, teniendo en cuenta al mismo tiempo los criterios de eficiencia y coherencia. Esta opción es también la que cuenta con el mayor apoyo de las partes interesadas.

¿Quién apoya cada opción?

La mayoría de las partes interesadas (privadas o públicas) coinciden en que es necesaria una actuación de la UE en pro de la resiliencia operativa de las empresas financieras. Muchas de ellas consideran también que la actuación de la UE es necesaria para poner fin a la carga normativa que supone el hecho de que las empresas financieras estén sujetas a normas duplicadas e incoherentes establecidas en la Directiva SRI, la legislación de la UE en materia de servicios financieros y los regímenes nacionales (por ejemplo, en lo que se refiere a la notificación de incidentes). Por consiguiente, son pocas las partes interesadas que se pronuncian a favor de no intervenir. Igualmente escasas son aquellas que consideran conveniente salvaguardar la resiliencia operativa mediante un aumento de los colchones de capital (opción 1). Sin embargo, este es el enfoque tradicional del riesgo operativo, en particular en el sector bancario, y, como tal, los organismos internacionales responsables de la elaboración de normas lo tienen en cuenta. El tipo de medidas cualitativas recogidas en la opción 2, que racionalizarían y modernizarían la legislación financiera de la UE y establecerían nuevos requisitos allí donde existan lagunas, manteniendo al mismo tiempo una vinculación con la Directiva SRI, de carácter horizontal, ha recibido un amplio apoyo de las partes interesadas que respondieron a la consulta pública. Si bien algunas de ellas (en particular las del sector público) consideran adecuado el refuerzo de la supervisión de los proveedores terceros de TIC contemplado en la opción 3, solo un número limitado apoya la creación a tal fin de una nueva autoridad de la UE, al igual que la ruptura más rotunda con el marco SRI.

C. Repercusiones de la opción preferida

¿Cuáles son las ventajas de la opción preferida (o, en su defecto, de las opciones principales)?

La opción 2 abordaría los **riesgos de TIC** en todo el sector financiero, mejorando la capacidad de resistencia de las entidades financieras ante incidentes de TIC. Se reduciría así el peligro de que un ciberincidente se propague rápidamente a través de los mercados financieros. Aunque es difícil estimar los costes de los incidentes operativos en el sector financiero (no todos los incidentes se notifican, y el alcance de los costes es incierto), las evaluaciones del sector sugieren que en la UE podrían oscilar entre 2 000 y 27 000 millones EUR al año. La opción preferida reduciría estos costes directos y cualquier repercusión más amplia que los ciberincidentes de mayor envergadura puedan tener para la estabilidad financiera. La supresión de los **requisitos de notificación** que se solapen reduciría las cargas administrativas. Por ejemplo, en el caso de algunos de los bancos más grandes, el correspondiente ahorro puede oscilar entre 40 y 100 millones EUR al año. La notificación directa también permitiría a los supervisores conocer mejor los incidentes de TIC. La realización de **pruebas armonizadas** aumentaría la detección de vulnerabilidades y riesgos desconocidos. Asimismo, reduciría los costes, especialmente para las empresas transfronterizas. Por ejemplo, en el caso de los 44 mayores bancos transfronterizos, se estima que los beneficios totales de un enfoque común en materia de pruebas podrían estar comprendidos entre los 11 millones y los 88 millones EUR. Mediante la introducción de un conjunto coherente de normas para la gestión de los riesgos de los **proveedores terceros de servicios de TIC**, las empresas financieras tendrían un mayor control sobre la manera en que los proveedores terceros cumplen el marco regulador, lo que podría acallar la posible inquietud de los supervisores. La vigilancia ejercida por los supervisores sobre los proveedores terceros de TIC también reportaría beneficios prudenciales. En términos generales, la opción preferida conlleva ventajas más amplias para la sociedad, derivadas de un entorno operativo más resiliente para todos los participantes en los mercados financieros y de una mayor protección de los consumidores y los inversores.

¿Cuáles son los costes de la opción preferida (o, en su defecto, de las opciones principales)?

La opción preferida daría lugar a costes puntuales y recurrentes. Los primeros se derivarían de las inversiones en sistemas informáticos y son difíciles de cuantificar, dado que la situación de los sistemas con que cuentan ya las empresas no es la misma. En ausencia de una intervención reguladora, algunas empresas financieras ya han realizado importantes inversiones en sistemas de TIC. Esto significa que, en el caso de las grandes empresas financieras, es probable que los costes ocasionados por la aplicación de las medidas de la presente propuesta sean reducidos. En el caso de las empresas más pequeñas, se espera que los costes sean también más bajos, ya que estarían sujetas a medidas menos estrictas, proporcionadas a su menor riesgo. Por lo que se refiere a las pruebas, las Autoridades Europeas de Supervisión han estimado que los costes relacionados con las pruebas de penetración basadas en las amenazas representan entre el 0,1 % y el 0,3 % del presupuesto total dedicado a las TIC de las empresas afectadas. Los costes relacionados con la notificación de incidentes se reducirían marcadamente, ya que no habría solapamientos con la notificación de la Directiva SRI. Los supervisores también incurrirían en algunos costes, debido a las tareas adicionales que asumirían. Por ejemplo, en el caso de aquellos que participen en la supervisión directa de proveedores terceros de TIC, el aumento estimado de los ETC podría ser de entre 1 y 5 ETC para la autoridad principal, y alrededor de 0,25 ETC para las autoridades participantes.

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

La opción preferida abarcaría a todas las empresas financieras, con el fin de aumentar la resiliencia operativa del sector en su conjunto. La amplitud del ámbito de aplicación es importante a la luz de la interconexión del sector financiero y de la correspondiente necesidad de contar, de forma general, con un buen grado de resiliencia operativa. Sin embargo, al definir los requisitos básicos en los principales ámbitos de intervención, el principio de proporcionalidad se aplicaría a todos los subsectores y dentro de cada subsector. Se tendrían en cuenta, entre otras cosas, las diferencias en los modelos de negocio, el tamaño, el perfil de riesgo, la importancia sistémica, etc. Por ejemplo, las medidas relativas a la notificación de incidentes y las pruebas serían menos estrictas para las empresas financieras más pequeñas.

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

No. Es posible que la supervisión adicional requiera, tal como se ha señalado anteriormente, un volumen limitado de recursos de supervisión adicionales, que podrían sufragarse total o parcialmente (si se cobran tasas de supervisión) con cargo a los presupuestos públicos.

¿Habrá otras repercusiones significativas?

Las consecuencias socioeconómicas de la pandemia de COVID-19 ilustran el carácter crítico de los mercados financieros digitales y de su resiliencia operativa. La opción preferida sentaría una base sólida para aprovechar la transformación digital, garantizando que el mercado único de servicios financieros, en particular en el marco de las uniones bancaria y de los mercados de capitales, sea resiliente desde el punto de vista operativo,

merced a un conjunto común de normas y requisitos encaminados a velar por la seguridad, el rendimiento, la estabilidad y unas condiciones de competencia equitativas. De este modo, se reforzará igualmente la posición de Europa como líder financiero y digital en el mundo, objetivo fijado por la Comisión en su Comunicación «Configurar el futuro digital de Europa».

D. Seguimiento

¿Cuándo se revisará la política?

La primera evaluación tendría lugar tres años después de la entrada en vigor del instrumento jurídico. La Comisión presentaría un informe al Parlamento Europeo y al Consejo sobre su revisión, la cual podría venir respaldada por una consulta pública, estudios, debates de expertos, encuestas o seminarios, según proceda.