

Bruxelas, 24.9.2020
SWD(2020) 199 final

DOCUMENTO DE TRABALHO DOS SERVIÇOS DA COMISSÃO

RELATÓRIO DO RESUMO DA AVALIAÇÃO DE IMPACTO

que acompanha o documento

Proposta de Regulamento do Parlamento Europeu e do Conselho

**relativo à resiliência operacional digital do setor financeiro e que altera os regulamentos
(CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014 e (UE) n.º 909/2014**

{COM(2020) 595 final} - {SEC(2020) 307 final} - {SWD(2020) 198 final}

Ficha de síntese
Avaliação de impacto sobre a proposta de regulamento relativo à resiliência operacional digital do setor financeiro
A. Necessidade de intervenção
Porquê? Qual é o problema em causa?
O setor financeiro depende em grande medida das tecnologias da informação e da comunicação (TIC). A atual pandemia de COVID-19 poderá intensificar esta dependência, tendo em conta os benefícios decorrentes da garantia de um acesso remoto e contínuo aos serviços financeiros. Contudo, a dependência das tecnologias digitais é motivo de preocupação; as empresas precisam de enfrentar as possíveis perturbações no domínio das TIC por forma a dar resposta às ameaças e aos incidentes digitais e a assegurar a continuidade dos seus serviços. Num setor financeiro extremamente interligado, que presta serviços transfronteiriços vitais para a economia real, as vulnerabilidades decorrentes da dependência das TIC, embora aplicáveis a todos os setores económicos, são especialmente acentuadas devido: 1) à intensiva e alargada utilização das TIC; e 2) à possibilidade de os efeitos de um incidente operacional numa empresa financeira ou subsetor financeiro se propagarem rapidamente a outras empresas ou partes do setor financeiro e, em última instância, ao resto da economia. Embora o setor financeiro esteja bastante avançado na sua integração de mercado e regulamentar e esteja a prosperar com base num conjunto único de regras harmonizadas – o conjunto único de regras da UE –, a resposta da UE face às necessidades acrescidas de resiliência operacional, tanto a nível horizontal como setorial: - tem vindo a basear-se numa harmonização mínima, deixando assim margem para interpretação nacional e fragmentação no mercado único, ou - tem sido demasiado geral e de aplicação limitada, dando resposta ao risco operacional global de forma variável, através da regulamentação parcial de alguns componentes de <i>resiliência</i> operacional digital (por exemplo, a gestão do risco associado às TIC, a comunicação de incidentes e o risco de terceiros no domínio das TIC), excluindo ao mesmo tempo outros elementos (realização de testes). Até à data, a intervenção da UE não deu resposta ao risco operacional de uma forma que satisfaça as necessidades das empresas financeiras no sentido de estas enfrentarem, responderem e recuperarem de vulnerabilidades no domínio das TIC. Também não fornece às autoridades de supervisão financeira as ferramentas necessárias para estas cumprirem o seu mandato de contenção da instabilidade financeira decorrente dessas vulnerabilidades no domínio das TIC. As lacunas e inconsistências atuais conduziram à proliferação de iniciativas nacionais não coordenadas (por exemplo, relativamente à realização de testes) e a abordagens de supervisão (por exemplo, dependências de terceiros no domínio das TIC) que se traduzem em sobreposições e duplicações de requisitos e em elevados custos administrativos e de conformidade para as empresas financeiras transfronteiriças, para além do problema dos riscos associados às TIC que continuam a não ser detetados nem abordados. De um modo geral, a estabilidade e a integridade do setor financeiro não estão garantidas e o mercado único dos serviços financeiros permanece fragmentado, enfraquecendo consequentemente a proteção de consumidores e investidores.
O que se espera alcançar com esta iniciativa?
O objetivo geral consiste em fortalecer a resiliência operacional digital do setor financeiro da UE através da simplificação e atualização da legislação financeira da UE existente e da introdução de novos requisitos onde existam lacunas, com vista a: • melhorar a gestão dos riscos associados às TIC pelas empresas financeiras; • aprofundar o conhecimento das autoridades de supervisão sobre as ameaças e os incidentes; • melhorar os testes pelas empresas financeiras dos seus sistemas de TIC; e • supervisionar de forma mais eficaz os riscos decorrentes da dependência das empresas financeiras em relação a entidades terceiras prestadoras de serviços no domínio das TIC. Mais concretamente, a proposta pretende criar mecanismos de comunicação de incidentes dotados de maior coerência e consistência, reduzindo assim os encargos administrativos para as instituições financeiras e aumentando a eficácia da supervisão.
Qual é o valor acrescentado da ação a nível da UE?
O mercado único dos serviços financeiros da UE é regido por um vasto conjunto de regras definidas a nível da UE, permitindo que as empresas financeiras autorizadas num Estado-Membro prestem serviços em todo o mercado único graças a um passaporte da UE. Consequentemente, as regras a nível nacional não constituiriam uma forma eficaz de reforçar a resiliência operacional das empresas financeiras que utilizem o passaporte.

Além disso, o conjunto único de regras da UE contém, em resultado da crise financeira, regras extremamente detalhadas e prescritivas que abordam os riscos mais «tradicionais», tais como os riscos de crédito, de mercado, de contraparte e de liquidez. As disposições existentes relativas ao risco operacional são pouco específicas. O reforço da resiliência operacional digital requer ajustes nas disposições relativas aos riscos operacionais que já se encontram definidas a nível da UE, pelo que apenas poderão ser atualizadas e complementadas a esse mesmo nível.

B. Soluções

Quais foram as opções legislativas e não legislativas ponderadas? É dada preferência a alguma das opções? Porquê?

A avaliação de impacto considerou três opções, além de um cenário de base em que não seriam tomadas medidas no que diz respeito à legislação da UE sobre os serviços financeiros. Mais especificamente:

- **«Nenhuma ação»:** as regras relativas à resiliência operacional continuariam a ser estabelecidas pelo atual conjunto divergente de disposições referentes aos serviços financeiros da UE, parcialmente pela Diretiva SRI e pelos regimes nacionais existentes ou futuros;
- **Opção 1 – reforço das reservas de capital:** seria introduzida uma reserva de capital adicional com vista a aumentar a capacidade das empresas financeiras para absorverem perdas que pudessem surgir devido à falta de resiliência operacional;
- **Opção 2 – um ato relativo à resiliência operacional digital dos serviços financeiros:** seria introduzido um quadro abrangente a nível da UE com regras referentes à resiliência operacional digital para todas as instituições financeiras, que permitiria
 - abordar os riscos associados às TIC de forma mais abrangente,
 - facilitar o acesso dos supervisores financeiros a informações sobre os incidentes relacionados com as TIC,
 - garantir que as empresas financeiras avaliam a eficácia das suas medidas preventivas e de resiliência e identificam as vulnerabilidades no domínio das TIC;
 - reforçar as regras de externalização que regem a fiscalização indireta das entidades terceiras prestadoras de serviços no domínio das TIC;
 - facilitar a fiscalização direta das atividades das entidades terceiras prestadoras de serviços no domínio das TIC sempre que prestem os seus serviços a empresas financeiras e,
 - adicionalmente, incentivar o intercâmbio de informações sobre as ameaças no setor financeiro.
- **Opção 3 – ato relativo à resiliência combinado com a supervisão centralizada das entidades terceiras prestadoras de serviços consideradas críticas:** além de um ato relativo à resiliência operacional (opção 2), seria criada uma nova autoridade com vista a supervisionar as entidades terceiras prestadoras de serviços considerados críticos no domínio das TIC a empresas financeiras. Delinearia igualmente de forma mais clara o setor financeiro no âmbito de aplicação da Diretiva SRI.

A opção 2 é a preferida. Em comparação com as outras opções, é aquela que permite atingir a maioria dos objetivos da iniciativa, tendo concomitantemente em conta os critérios da eficiência e da coerência. Esta opção é também a mais apoiada pelas partes interessadas.

Quem apoia cada uma das opções?

A maioria das partes interessadas (privadas e públicas) aceita que a ação da UE é necessária por forma a melhor salvaguardar a resiliência operacional das empresas financeiras. Várias acreditam que a ação da UE é necessária para dar resposta aos encargos regulamentares decorrentes do facto de as empresas financeiras estarem sujeitas a regras duplicadas e inconsistentes estabelecidas na Diretiva SRI, em legislação relativa aos serviços financeiros da UE e em regimes nacionais (por exemplo, no que diz respeito à comunicação de incidentes). Em conformidade, poucas partes interessadas apoiam a opção «Nenhuma ação». Poucas partes interessadas veem vantagens em garantir a resiliência operacional através do aumento das reservas de capital (opção 1). De qualquer modo, esta é a abordagem tradicional face ao risco operacional, nomeadamente no setor bancário, e é, como tal, considerada pelos organismos de normalização internacionais, por exemplo. O tipo de medidas qualitativas definidas na opção 2 que irão simplificar e atualizar a legislação financeira da UE e introduzir novos requisitos onde existam lacunas, mantendo simultaneamente as ligações à Diretiva horizontal SRI, reúne o apoio alargado das partes interessadas que responderam à consulta pública. Enquanto algumas partes interessadas (nomeadamente públicas) veem vantagens na supervisão reforçada das entidades terceiras prestadoras de serviços no domínio das TIC prevista na opção 3, a criação de uma nova autoridade para esse fim apenas tem um apoio limitado das partes interessadas, tal como uma rutura mais completa com o quadro da Diretiva SRI.

C. Impacto da opção preferida
Quais são os benefícios da opção preferida (se existir; caso contrário, das principais opções)?
A opção 2 irá abordar os riscos associados às TIC no setor financeiro através da melhoria das capacidades das instituições financeiras para enfrentarem os incidentes no domínio das TIC. Tal reduzirá o risco de um incidente cibernético se disseminar rapidamente nos mercados financeiros. Embora seja difícil estimar os custos dos incidentes operacionais no setor financeiro (nem todos os incidentes são comunicados; âmbito dos custos incerto), as avaliações do setor sugerem que os custos para o setor financeiro da UE podem variar entre 2 e 27 mil milhões de EUR por ano. A opção preferida irá atenuar esses custos diretos e quaisquer impactos mais vastos que incidentes cibernéticos graves possam ter na estabilidade financeira. A eliminação da sobreposição de requisitos de comunicação reduzirá os encargos administrativos. Para alguns dos maiores bancos, por exemplo, as poupanças associadas podem variar entre 40 e 100 milhões de EUR por ano. A comunicação direta de informações também aprofundará o conhecimento das autoridades de supervisão sobre os incidentes no domínio das TIC. As práticas de testes harmonizados melhorarão a deteção de vulnerabilidades e riscos desconhecidos. Tal reduzirá também os custos, principalmente para as empresas transfronteiriças. Para os 44 maiores bancos transfronteiriços, por exemplo, os benefícios totais previstos de uma abordagem comum de realização de testes poderão variar entre 11 e 88 milhões de EUR. Com a introdução de um conjunto coerente de regras em matéria de gestão dos riscos de entidades terceiras prestadoras de serviços no domínio das TIC, as empresas financeiras poderão controlar melhor o modo como essas entidades terceiras prestadoras de serviços cumprem o quadro regulamentar, o que permitirá tranquilizar as autoridades de supervisão. Existirão ainda benefícios prudenciais decorrentes da fiscalização da supervisão de entidades terceiras prestadoras de serviços no domínio das TIC. De modo geral, a opção preferida traduz-se em benefícios societais mais abrangentes, decorrentes de um ambiente operacional mais resiliente para todos os participantes do mercado financeiro e da proteção reforçada do consumidor e do investidor.
Quais são os custos da opção preferida (se existir; caso contrário, das principais opções)?
A opção preferida dará origem a custos pontuais e recorrentes. Os primeiros, estes devem-se aos investimentos em sistemas de TI e são difíceis de quantificar, tendo em conta o diferente estado dos sistemas preexistentes das empresas. Na ausência de uma intervenção regulamentar, algumas empresas financeiras já investiram consideravelmente em sistemas de TIC. Tal significa que, para as grandes empresas financeiras, os custos de aplicação das medidas da presente proposta serão provavelmente reduzidos. Para empresas de menor dimensão, prevê-se que os custos também sejam inferiores, uma vez que estarão sujeitas a medidas menos rigorosas, proporcionadas ao menor risco que representam. No que se refere à realização de testes, as Autoridades Europeias de Supervisão preveem que os custos relacionados com a realização de testes de penetração motivados por ameaças variem entre os 0,1 % e os 0,3 % do orçamento total no domínio das TIC das empresas envolvidas. Os custos relacionados com a notificação de incidentes serão drasticamente reduzidos, visto que deixará de haver sobreposições com a comunicação de informações no âmbito da Diretiva SRI. Os supervisores também incorrerão nalguns custos devido às tarefas adicionais que assumirão. No caso dos supervisores que participem na fiscalização direta de entidades terceiras prestadoras de serviços no domínio das TIC, por exemplo, o aumento estimado em equivalentes a tempo inteiro (ETI) poderá variar entre 1 e 5 ETI para a autoridade principal e cerca de 0,25 ETI para as outras autoridades participantes.
Como serão afetadas as empresas, as PME e as microempresas?
A opção preferida irá abranger todas as empresas financeiras, com vista a aumentar a resiliência operacional da totalidade do setor. Este âmbito abrangente é importante à luz da natureza interligada do setor financeiro e da necessidade correspondente de assegurar um nível elevado de resiliência operacional global. No entanto, e no que respeita à definição dos requisitos principais em todas as principais áreas de intervenção, o princípio da proporcionalidade será aplicável a todos os subsectores, bem como no interior de cada um dos subsectores. Serão tidas em conta, entres outras, as diferenças em termos de modelo empresarial, dimensão, perfil de risco, importância sistémica, etc. As medidas referentes à comunicação de incidentes e à realização de testes, por exemplo, serão menos rigorosas para as empresas financeiras de menor dimensão.
Haverá impactos significativos nos orçamentos e administrações públicas nacionais?
Não. A fiscalização adicional pode, conforme demonstrado anteriormente, exigir um nível limitado de recursos de supervisão adicionais, que poderão ter de ser total ou parcialmente (se existirem taxas de supervisão) suportados pelos orçamentos públicos.
Haverá outros impactos significativos?
As consequências socioeconómicas da pandemia de COVID-19 ilustram a natureza crítica dos mercados financeiros digitais e da sua resiliência operacional. A opção preferida estabelecerá uma base sólida com vista

a aproveitar a transformação digital, assegurando a resiliência operacional do mercado único dos serviços financeiros, incluindo o setor bancário e a união dos mercados de capitais, com base num conjunto comum de regras e requisitos que visam a segurança, o desempenho, a estabilidade e condições equitativas. Tal irá também reforçar a posição da Europa enquanto líder financeiro e digital no mundo, um objetivo estabelecido pela Comissão na sua Comunicação «Construir o futuro digital da Europa».

D. Acompanhamento

Quando será revista a política?

A primeira revisão deverá ter lugar três anos após a entrada em vigor do instrumento jurídico. A Comissão deverá apresentar ao Parlamento Europeu e ao Conselho um relatório relativo à sua revisão nesse contexto. A revisão poderá ser fundamentada através de consultas públicas, estudos, discussões de peritos, inquéritos ou seminários, consoante o caso.