Conselho da
União Europeia

**Bruxelas, 18 de dezembro de 2020**
**(OR. en)**

**14150/20**
**ADD 3**

**Dossiê interinstitucional:**
**2020/0359 (COD)**

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

**NOTA DE ENVIO**

| | |
|---|---|
| de: | Secretária-geral da Comissão Europeia, com a assinatura de Martine DEPREZ, diretora |
| data de receção: | 16 de dezembro de 2020 |
| para: | Jeppe TRANHOLM-MIKKELSEN, Secretário-Geral do Conselho da União Europeia |
| n.° doc. Com.: | SWD(2020) 344 final |
| Assunto: | DOCUMENTO DE TRABALHO DOS SERVIÇOS DA COMISSÃO RELATÓRIO DO RESUMO DA AVALIAÇÃO DE IMPACTO que acompanha o documento Proposta de Diretiva do Parlamento Europeu e do Conselho relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União e que revoga a Diretiva (UE) 2016/1148 |

Envia-se em anexo, à atenção das delegações, o documento SWD(2020) 344 final.

Anexo: SWD(2020) 344 final

COMISSÃO
EUROPEIA

Bruxelas, 16.12.2020
SWD(2020) 344 final

# DOCUMENTO DE TRABALHO DOS SERVIÇOS DA COMISSÃO

# RELATÓRIO DO RESUMO DA AVALIAÇÃO DE IMPACTO

***que acompanha o documento***

**Proposta de Diretiva do Parlamento Europeu e do Conselho**

**relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União e que revoga a Diretiva (UE) 2016/1148**

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

**Ficha de síntese**

Avaliação de impacto sobre a *Revisão da Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União (a seguir designada por «Diretiva SRI»)*

## A. Necessidade de agir

### Qual o problema e por que tem dimensão europeia?

Apesar dos seus resultados extraordinários, a Diretiva SRI, que abriu as portas a uma mudança significativa das mentalidades em relação à abordagem institucional e regulamentar à cibersegurança em muitos Estados-Membros, também já deixou bem claras as suas limitações. A transformação digital da sociedade (intensificada pela crise da COVID-19) ampliou o cenário de ameaças e está a gerar novos desafios, que requerem respostas adaptadas e inovadoras. O número de ciberataques continua a aumentar, com ataques cada vez mais sofisticados provenientes de uma grande variedade de fontes dentro e fora da UE.

Com base na avaliação da aplicação da Diretiva SRI, a avaliação de impacto identificou os seguintes problemas: o baixo nível de ciber-resiliência das empresas que operam na UE; as diferenças em termos de resiliência entre Estados-Membros e setores; e o baixo nível de conhecimento situacional comum e a inexistência de mecanismos de resposta conjunta a situações de crise. Por exemplo, como resultado de alguns destes problemas e fatores, existem situações em que alguns dos principais hospitais num Estado-Membro não estão abrangidos pelo âmbito da Diretiva SRI e, como tal, não estão obrigados a aplicar as medidas de segurança nela previstas, ao passo que, noutro Estado-Membro, praticamente todos os hospitais do país estão sujeitos aos requisitos de segurança estabelecidos nessa diretiva.

### Quais são os resultados esperados?

A revisão da Diretiva SRI visa três objetivos gerais:

1. **Aumentar o nível de ciber-resiliência de um conjunto abrangente de empresas que operam na União Europeia em todos os setores importantes,** estabelecendo regras que assegurem que todas as entidades públicas e privadas em todo o mercado interno, que desempenham funções importantes para a economia e a sociedade no seu conjunto, sejam obrigadas a tomar medidas de cibersegurança adequadas;

2. **Reduzir as diferenças em termos de resiliência no mercado interno nos setores já abrangidos pela diretiva,** por via de uma maior harmonização: 1) do âmbito de aplicação efetivo, 2) dos requisitos em matéria de segurança e de comunicação de incidentes, 3) das disposições que regem a supervisão e a execução coerciva a nível nacional, 4) das capacidades das autoridades competentes dos Estados-Membros;

3. **Melhorar o nível de conhecimento situacional comum e a capacidade coletiva de preparação e resposta,** tomando medidas para aumentar o nível de confiança entre as autoridades competentes, partilhando mais informações, e estabelecendo regras e procedimentos em caso de um incidente ou crise em grande escala.

### Qual é o valor acrescentado da ação a nível da UE (subsidiariedade)?

A ciber-resiliência não pode ser eficaz em toda a União se for abordada de forma díspar por via de

medidas nacionais ou regionais estanques. A Diretiva SRI surgiu para colmatar esta lacuna, estabelecendo um quadro para a segurança das redes e dos sistemas de informação a nível nacional e da União. Porém, a sua transposição e aplicação revelaram também as deficiências inerentes a determinadas disposições ou abordagens, como a falta de clareza na definição do âmbito da Diretiva SRI. Acresce que, desde o início da crise da COVID-19, a economia europeia está mais dependente do que nunca das redes e dos sistemas de informação, e a interligação entre setores e serviços é cada vez maior. A primeira avaliação periódica da Diretiva SRI criou, assim, uma oportunidade para novas ações da UE. A intervenção da UE, indo além das atuais medidas previstas na Diretiva SRI, justifica-se principalmente: i) pelo carácter transfronteiriço do problema; ii) pelo potencial da ação da UE para melhorar e facilitar a eficácia das políticas nacionais; iii) pelo contributo de ações concertadas e colaborativas de política em matéria de SRI para uma proteção eficaz dos dados e da privacidade.

**B. Soluções**

**Quais são as várias opções para cumprir os objetivos? Há alguma opção preferida? Em caso negativo, por que razão?**

A avaliação de impacto analisou quatro opções políticas: 0) manutenção do *status quo*; 1) medidas não legislativas para alinhar a transposição; 2) alterações limitadas da Diretiva SRI para uma maior harmonização; 3) alterações sistémicas e estruturais da Diretiva SRI. A opção 1 foi descartada numa fase inicial, uma vez que não se afasta consideravelmente do *status quo*. A avaliação de impacto conclui que a **opção preferida** é a opção 3 (ou seja, **alterações sistémicas e estruturais do quadro para a SRI**), dado que contemplaria uma mudança de abordagem mais profunda no sentido de abranger um segmento mais alargado das economias da União, embora com uma supervisão mais direcionada para as empresas proporcionalmente maiores e fundamentais, determinando, ao mesmo tempo e de forma clara, o âmbito de aplicação. Além disso, simplificaria as obrigações impostas às empresas no domínio da segurança e reforçaria a sua harmonização, criaria um panorama mais eficaz para os aspetos operacionais, estabeleceria uma base clara para a partilha de responsabilidades e para a responsabilização dos intervenientes, e incentivaria a partilha de informações.

**Quais são as perspetivas dos vários intervenientes? Quem apoia cada uma das opções?**

A maioria das empresas e autoridades competentes demonstraram apoio a uma revisão da Diretiva SRI. Ao longo de várias consultas, referiram que uma Diretiva SRI revista deveria abranger (sub)setores adicionais, bem como aumentar a harmonização ou simplificação das medidas de segurança e das obrigações de notificação. Os intervenientes também demonstraram apoio a novos conceitos ou medidas relacionadas com políticas que apenas constam da opção preferida (por exemplo, políticas de segurança das cadeias de abastecimento, institucionalização de um quadro operacional de gestão de crises da UE).

**C. Impactos da opção preferida**

**Quais os benefícios da opção preferida (se existir; caso contrário, das principais opções)?**

A opção preferida traria benefícios significativos: as estimativas feitas com base numa modelização económica desenvolvida por um estudo de apoio à revisão da Diretiva SRI indicam que a opção preferida pode levar a uma redução do custo dos incidentes de cibersegurança de 11 300 milhões de EUR.

O âmbito setorial seria consideravelmente alargado ao abrigo do quadro para a SRI, mas, além dos benefícios acima referidos, os encargos que poderão resultar dos requisitos de SRI, nomeadamente do ponto de vista da supervisão, também seriam equilibrados, tanto para as novas entidades a abranger como para as autoridades competentes, uma vez que o novo quadro para a SRI estabeleceria uma abordagem de

dois níveis, centrada em entidades grandes e fundamentais, e uma diferenciação do regime de supervisão que permite apenas a supervisão *ex post* (ou seja, reativa e sem uma obrigação geral de documentar sistematicamente o cumprimento) para um grande número dessas entidades, nomeadamente as consideradas «importantes», mas não «essenciais».

No geral, a opção política preferida levaria a sinergias e soluções de compromisso eficientes, tendo o maior potencial, de entre todas as opções analisadas, para assegurar um nível de ciber-resiliência acrescido e coerente das entidades fundamentais em toda a União, que acabaria por originar uma poupança de custos tanto para as empresas como para a sociedade.

**Quais são os custos da opção preferida (se existir; caso contrário, das principais opções)?**

A opção política preferida acarretaria determinados custos de conformidade e de execução coerciva para as autoridades competentes dos Estados-Membros (estima-se um aumento global de cerca de 20 % a 30 % dos recursos). No entanto, o novo quadro também traria benefícios substanciais decorrentes de uma melhor panorâmica das principais empresas e de uma interação acrescida com as mesmas, de um reforço da cooperação operacional transfronteiriça, e de mecanismos de assistência mútua e de análise pelos pares. Tal levaria a um reforço global das capacidades de cibersegurança em todos os Estados-Membros.

No respeitante às empresas que ficariam abrangidas pelo âmbito de aplicação do quadro para a SRI, estima-se que precisariam de um aumento máximo de 22 % das suas atuais despesas com segurança das TIC durante os primeiros anos após a sua introdução (que seria de 12 % para as empresas já abrangidas pelo âmbito de aplicação da atual Diretiva SRI). No entanto, este aumento médio das despesas com a segurança das TIC levaria a um benefício proporcional de tais investimentos, nomeadamente devido a uma redução considerável do custo dos incidentes de cibersegurança (estimada em 11 300 milhões de EUR em dez anos).

**Quais são os efeitos para as PME e a competitividade?**

Nos termos da opção preferida, as pequenas e microempresas ficariam isentas do âmbito do quadro para a SRI. No caso das médias empresas, verificar-se-ia provavelmente um aumento do nível das despesas com a segurança das TIC nos primeiros anos após a introdução do novo quadro para a SRI. Ao mesmo tempo, o reforço dos requisitos de segurança para estas entidades fomentaria também as suas capacidades de cibersegurança e ajudaria a melhorar a sua gestão dos riscos associados às TIC.

**Haverá impactos significativos nos orçamentos e nas administrações públicas nacionais?**

Haveria um impacto nos orçamentos e nas administrações públicas nacionais: seria de esperar um aumento estimado de aproximadamente 20 % a 30 % dos recursos a curto e médio prazo.

**Haverá outros impactos significativos?**

Não são esperados outros impactos negativos significativos. Espera-se que a opção política preferida dê origem a capacidades mais sólidas em matéria de cibersegurança e, consequentemente, tenha um impacto atenuante mais substancial no número e na gravidade dos incidentes, incluindo das violações de dados. É também provável que tenha um impacto positivo na garantia de condições de concorrência equitativas em todos os Estados-Membros para as entidades abrangidas pelo âmbito da Diretiva SRI, e que reduza as assimetrias em termos de informações sobre cibersegurança.

**Proporcionalidade?**

| |
|---|
| A opção preferida não excede o estritamente necessário para atingir os objetivos específicos de forma satisfatória. A harmonização e a racionalização previstas das medidas de segurança e das obrigações de notificação estão relacionadas com os pedidos formulados pelos Estados-Membros e pelas empresas para melhorar o quadro atual. |
| **D. Acompanhamento** |
| **Quando será revista a política?** |
| A primeira revisão teria lugar 54 meses após a entrada em vigor do instrumento jurídico. A Comissão apresentaria um relatório ao Parlamento Europeu e ao Conselho relativo à sua revisão, que seria realizada com o apoio da ENISA e do grupo de cooperação. |