DIGITALEUROPE

# Transposição da Diretiva Relativa à Segurança das Redes e da Informação (SRI) da UE

*Bruxelas*, 5 July 2016

## RESUMO EXECUTIVO

O Conselho da União Europeia publicou a versão final da Diretiva Relativa à Segurança das Redes e da Informação (SRI) da UE a 21 de abril de 2016. Enquanto isso precisa ser formalmente aprovada pelo Parlamento Europeu durante o verão, o texto em si foi acordado entre as três instituições da União Europeia e não se espera que venha a ser alterado. Os Estados-Membros estão obrigados a transpô-lo para o direito nacional no prazo de 21 meses após a sua adoção. Para facilitar este processo, poderá encontrar em anexo as melhores práticas recomendadas para implementar os aspetos relevantes para a indústria da tecnologia e consagrar de forma efetiva as intenções dos redatores.

A Diretiva SRI da UE é a primeira legislação a nível europeu sobre a segurança cibernética e concentra-se no reforço das autoridades cibernéticas a nível nacional, aumentando a coordenação entre elas e introduzindo requisitos de segurança para os setores-chave da indústria.

Qualquer legislação de implementação nacional não deve perder de vista os dois principais objetivos da Diretiva: (1) assegurar uma segurança cibernética de alto nível para as infraestruturas críticas do país; (2) estabelecer um mecanismo de cooperação eficaz entre os Estados-Membros da UE para promover este objetivo. Os recursos devem serem primeiro lugar, e acima de tudo, dedicados a alcançar estes dois objetivos importantes.

**Para a indústria da tecnologia, as disposições relativas aos chamados prestadores de serviços digitais (PSDs) são de particular interesse.** A Diretiva estabelece claramente que existem diferenças fundamentais entre os operadores de serviços essenciais (OSEs) e os PSDs. De facto, estes últimos não devem ser considerados estruturas críticas como tal. Como a legislação reconhece, um incidente com impacto nestes serviços digitais seria responsável por um nível significativamente mais baixo de risco para a segurança económica de um país e para a segurança pública. Manter esta distinção é essencial também para, de forma eficaz e eficiente, implementar os recursos escassos das autoridades que terão de supervisionar e fazer cumprir as regras.

Deste modo, chamamos a atenção para o âmbito pretendido dos serviços em causa e pedimos aos formuladores de políticas que não sujeitem setores, outros do que aqueles identificados como PSDs e OSEs, aos requisitos de segurança na legislação nacional.

No que diz respeito à jurisdição, os PSDs devem poder depender da legislação aplicável no país do seu estabelecimento principal, mesmo nos casos em que estejam envolvidas as autoridades competentes de mais do que um país. Relativamente à supervisão, as autoridades competentes devem seguir uma abordagem ex-post, em oposição à imposição de uma obrigação geral para supervisionar os PSDs. Além disso, devem concentrar-se nos resultados e manter a distinção entre OSEs e PSDs não submetendo estes últimos a exigências não previstas pela Diretiva como, por exemplo, a auditoria e instruções vinculativas.

DIGITALEUROPE
Rue de la Science, 14 - 1040 Bruxelas [Bélgica]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Membro do registo de transparência para a Comissão: 64270747023-20

As Medidas de segurança relativamente aos PSDs devem ser diferentes do que para os OSEs, visto que a Diretiva afirma que estas representam um risco de segurança significativamente menor. Os decisores devem entender o objetivo de harmonização relativamente a estes serviços, reconhecer os padrões internacionais existentes conduzidos pela indústria, evitar mandatos tecnológicos e respeitar o direito dos PSDs consagrados na Diretiva de definir medidas de segurança mais adequadas para os seus sistemas. As comunicações de incidentes também devem ser harmonizadas quanto possível a nível europeu, e deverão concentrar-se em incidentes que afetem a continuidade do serviço, respeitar a flexibilidade quanto ao momento da notificação e criar um ambiente de confiança que incentive a partilha de informações sem expor a parte notificante a um aumento da responsabilidade

As medidas impostas a OSEs também terão impacto noutras indústrias visto que as medidas de segurança e comunicação de incidentes irão refletir-se nas disposições contratuais. Isto é particularmente verdadeiro para os serviços ' cloud'.. Como resultado, os PSDs podem estar indiretamente sujeitos às leis nacionais dos seus clientes e, assim sendo, temos um grande interesse em ver medidas de segurança reconhecidas internacionalmente aplicadas a esses serviços. Propomos também uma coordenação e sinergias tanto quanto possível, entre os requisitos de informação, tanto relativamente aos OSEs como aos PSDs, dado que os últimos são suscetíveis de ser objeto de notificação dupla.

A Diretiva estabelece a ambição de alcançar um nível comum elevado de segurança das redes e sistemas de informação para melhorar o funcionamento do mercado interno. Para alcançar este nobjetivo elevado, as transposições nacionais devem concentrar-se numa estratégia baseada no risco, harmonizada e internacional que conceda aos intervenientes do setor privado a flexibilidade para se adaptarem a um cenário de ameaças em constante mudança, permita às autoridades cibernéticas concentrar os seus recursos limitados nos desafios mais significativos e reconhecer que a solução para um problema sem fronteiras necessita de ser global. Esperamos que que essa orientação é útil para esse fim. Teríamos o maior prazer em responder a quaisquer perguntas que possa ter.

# Anexo: Melhores Práticas Recomendadas para a Implementação da Diretiva SRI

## 1. Prestadores de serviços digitais

### a) Âmbito

- A Diretiva determina que os mercados online, os motores de busca online e os serviços informáticos em nuvem devem ser considerados prestadores de serviços digitais (PSDs) e, portanto, incluídos no âmbito da Diretiva. Ao passo que esta é uma Diretiva de harmonização mínima (Artigo 2º), é importante para manter a coerência em toda a UE e, portanto, os Estados-Membros não devem sujeitar setores que não os identificados como PSDs ou operadores de serviços essenciais (OSEs) - conforme definido no Artigo 3 - aos requisitos de segurança na legislação nacional.

- A Diretiva estabelece explicitamente que os fabricantes de hardware e os desenvolvedores de software não são OSEs nem PSDs e que, portanto, não devem ser abrangidos pelas leis nacionais de transposição da Diretiva (Considerando 50).

- A Diretiva exclui expressamente do âmbito de mercados online serviços online que atuem como intermediários de serviços de terceiros onde o contrato de serviço ou vendas é finalmente concluído (por exemplo, sites de comparação) (Considerando 15).

- As funções de pesquisa limitadas ao conteúdo de um site específico não devem ser tratadas como motores de busca online, mesmo que façam uso de um fornecedor externo (Considerando 16).

- A definição de um serviço informáticos em nuvem no âmbito da Diretiva depende dos recursos informáticos partilhados pelos vários utilizadores (Artigo 4 (19) e Considerando 17). Dado que as nuvens privadas (ao contrário das nuvens públicas) são dedicadas a uma única organização, estas não devem ser abrangidas.

- A Diretiva sublinha que existem diferenças fundamentais entre OSEs e PSDs, e é por esta razão que os PSDs estão sujeitos a regras diferentes (Considerando 57). Tal distinção deverá ser mantida ao implementar a Diretiva.

### b) Jurisdição e supervisão

- A jurisdição relativamente aos PSDs deve ser atribuída a um único Estado-Membro, onde o operador tenha o seu principal estabelecimento na UE que, em princípio, corresponde ao local onde tem a sua sede na UE (Artigo 18.1 e Considerando 64). Defendemos que os PSDs devem fazer uma tal determinação eles próprios e que esta decisão só poderá estar sujeita a revisão caso as autoridades competentes a contestem na circunstância de ações de supervisão ex-post.

- Sempre que os PSDs tenham sistemas de redes e informação noutros países que não o local do seu estabelecimento principal, o Artigo 17.3 prevê que as autoridades competentes cooperem. No entanto, do ponto de vista dos PSDs, é importante que a lei aplicável permaneça a do país do seu estabelecimento

principal e que permaneçam unicamente responsáveis perante a autoridade competente nessa jurisdição, que funcionará como seu interlocutor.

- A Diretiva sublinha que os PSDs estão sujeitos a supervisão ex-post reativa e que, consequentemente, as autoridades competentes não têm qualquer obrigação geral de supervisionar os PSDs só devendo agir quando na posse de provas. (Artigo 17.1 e Considerando 60). Estas disposições devem ser respeitadas ao aplicar a diretiva.

- Ao contrário dos OSEs, no caso dos PSDs as autoridades só podem solicitar informações e exigir que os PSDs corrijam qualquer falha. A Diretiva torna claro que as autoridades não têm poderes de auditoria e não podem emitir instruções vinculativas. Estas disposições devem também ser respeitadas a nível nacional.

## c) Requisitos adicionais

- Os requisitos de segurança e notificação dos PSDs estão sujeitos a harmonização máxima (Artigo 16.10). Este Artigo deve ser tido em consideração para aplicação aos produtos, serviços e soluções que compõem as suas redes e sistemas de informação. Como resultado, as disposições adicionais como, por exemplo, testes de produtos, não devem ser necessárias na medida em que os produtos e serviços são utilizados neste contexto.

## d) Medidas de Segurança e Normas

- As medidas de segurança para os PSDs devem ser mais leves que as dos OSEs. Os PSDs devem ser livres para definir a forma como implementam a segurança e como pretendem assegurar a proteção das suas redes e sistemas de informação tendo em conta os riscos apresentados (Considerando 49).

- As medidas de segurança devem ser orientadas para o processo e concentrar-se na gestão de riscos. Estas não devem exigir que os produtos de TIC sejam concebidos, desenvolvidos ou fabricados de forma específica (Considerando 51).

- A Diretiva sublinha que os Estados-Membros não devem impor quaisquer requisitos adicionais de segurança aos PSDs (Artigo 16.10).

- No entanto, aguardamos diretrizes de vários intervenientes. Os Estados-Membros garantirão que as medidas referidas na Diretiva são adotadas (Artigo 16.1), podem encorajar a utilização de normas para a sua implementação (Artigo 19.1) e discutir as normas com os Organismos Europeus de Normalização no Grupo de Cooperação (Artigo 11.3 (h)). A ENISA dará conselhos relativamente às normas adequadas (Artigo 19.2) e a Comissão Europeia está incumbida de adotar atos de implementação relativamente às medidas de segurança (Artigo 16.8).

- Dado este nível de complicação e os benefícios da harmonização, aconselhamos que os processos nacionais devem essencialmente adiar o processo para os atos de implementação para acordar medidas adequadas, o que em qualquer caso terá de ser finalizado no prazo de um ano após a adoção da Diretiva.

Os atos de implementação em si não deverão prejudicar a capacidade dos PSDs para definir as medidas de segurança mais adequadas para os seus sistemas.

- O Artigo sobre as normas permite que as normas europeias ou internacionalmente aceites sejam referenciadas (Artigo 19.1). Dada a maturidade das normas internacionais em vigor nesta área, recomendamos que, sempre que existam normas apropriadas, a certificação de uma delas (como a ISO 27001) seja suficiente para cumprir os requisitos.

- Em qualquer caso, a certificação das normas deve ser facultativa e não obrigatória. O Artigo 19 salienta que qualquer norma só pode ser "encorajada" e que esta deverá sê-lo "sem que se façam imposições ou discriminações a favor da utilização de um determinado tipo de tecnologia."

## e) Relatórios de Incidentes de Segurança

- Tal como acontece com as medidas de segurança, múltiplas partes desempenham um papel na elaboração de relatórios de incidentes ao abrigo da Diretiva SRI. Os Estados-Membros devem garantir que os PSDs enviam uma notificação relativa a tais incidentes de segurança com impacto significativo no serviço (que está no âmbito da Diretiva) que prestam (Artigo 16.3), o Grupo de Cooperação está encarregado de discutir as modalidades de notificação (Artigo 11.3(m)) e a Comissão de adotar atos de implementação (Artigos 16.8 e 9).

- Mais uma vez, a nossa recomendação é que as transposições nacionais adiem o processo para os atos de implementação, dos quais o ato de implementação sobre o limiar de notificação deverá ser adotado no prazo de um ano após a conclusão da Diretiva.

- No que toca aos tipos de incidente que devem ser reportados, os PSDs estão incumbidos de notificar "qualquer incidente com impacto substancial no fornecimento do [seu] serviço" (Artigo 16.3). Quanto à aplicação das disposições equivalentes para os operadores de telecomunicações ao abrigo do Artigo 13a da Diretiva-Quadro, acreditamos que este deve ser interpretado de forma a concentrar-se na **continuidade (ou disponibilidade)** dos serviços prestados. Por outras palavras, as interrupções que atinjam um determinado limite (a determinar através dos atos de implementação) devem ser relatadas em detrimento de qualquer outro tipo de incidente de segurança. Tal tem a vantagem de se concentrar nos incidentes com maior probabilidade de ter impacto na economia ou na sociedade, minimizando (embora não inteiramente eliminando) a sobreposição com os requisitos de notificação de violação de dados pessoais decorrentes do Regulamento Geral de Proteção de Dados.

- Além disso, a obrigação de elaboração de relatórios de "Operadores de Serviços Essenciais" especifica que estes operadores devem notificar "incidentes com impacto significativo na continuidade dos serviços essenciais que prestam", o que tem um foco claro na continuidade (ou disponibilidade) do serviço. Os colegisladores concordaram que as obrigações dos PSDs devem ser mais leves que as dos OSEs (ver Considerando 49). A obrigação de comunicação de incidentes dos PSDs no âmbito do NIS não deverá ser, portanto, mais ampla do que a dos OSEs; na verdade, deveria ser ainda mais restritiva em termos de limites. Isto, mais uma vez, reforça o facto de que a elaboração de relatórios para os PSDs deverá estar limitada a incidentes que atinjam um limite específico e **afetem a continuidade/disponibilidade do serviço** e não incidentes relacionados com a integridade ou

confidencialidade dos dados, o que em grande medida já está coberto pelos requisitos de notificação relacionados nos termos da regulamentação PIBR e eIDAS.

- Em relação ao momento da notificação, apreciamos a flexibilidade subentendida na linguagem do relatório "sem demora indevida" (Artigo 16.3). A implementação não deve originar prazos rígidos visto que os incidentes variam significativamente em termos de complexidade. Momentos uniformes de apresentação de relatórios originariam uma notificação imprecisa sempre que o âmbito inicial dos sistemas afetados não fosse claro e teria impacto na capacidade dos profissionais que respostem a incidentes de definir prioridades ao responder ao incidente em oposição à elaboração de relatórios sobre o mesmo.

- Como discutido, os incidentes de segurança notificados ao abrigo da Diretiva podem também exigir uma notificação ao abrigo da legislação de proteção de dados, dependendo se a informação pessoal é violada. Isto significa não só comunicar o mesmo incidente a diferentes autoridades, mas tais autoridades podem até estar em diferentes Estados-Membros dependendo da jurisdição aplicável ao PSD de acordo com a legislação dos Estados-Membros. Recomendamos que os Estados-Membros reconheçam a necessidade e se esforcem no sentido da notificação única de incidentes, e ainda que procurem criar canais de comunicação para partilhar informações relevantes entre eles, sem prejuízo do sigilo comercial.

- As autoridades competentes devem ter em conta as implicações comerciais e reputacionais para os PSDs antes de partilharem publicamente informações sobre incidentes. Acima de tudo, divulgar o incidente poderia aumentar o risco de segurança. Desta forma, é importante coordenar com os intervenientes em questão antes de qualquer divulgação.

- A Diretiva sublinha que a informação considerada confidencial deve ser tratada como tal (Considerandos 41, 59, Artigo 1.5).

- O Artigo 16.3 sublinha que a notificação de incidente de segurança não deverá expor a parte notificante a um aumento da responsabilidade.

## 2. Operadores essenciais

### a) Aplicação alargada de medidas de segurança

- Os PSDs que tenham OSEs como clientes estarão sujeitos a medidas de segurança aplicáveis que provêm de negociações contratuais provenientes das obrigações legais relacionadas com os operadores essenciais (Artigo 14.1). Como tal, podem estar indiretamente sujeitos à legislação nacional dos seus clientes, independentemente da lei aplicável no país da sua sede europeia.

- Como resultado, os esforços para harmonizar as medidas de segurança para os operadores essenciais seriam bem-vindos. Apesar de os Estados-Membros terem o direito de impor obrigações mais rigorosas aos operadores essenciais que as indicadas no âmbito da Diretiva (Artigo 3º), recomendamos restrição ao fazê-lo e incentivamos os Estados-Membros a trabalhar no sentido de uma abordagem harmonizada. Tal poderia ser alcançado evitando medidas adicionais em transposições nacionais e procurando

determinar medidas de segurança apropriadas no Grupo de Cooperação ao invés de se optar por uma focagem no processo nacional.

- Os requisitos de segurança devem, tanto quanto possível, basear-se em normas internacionais (como a série ISO 27x) e nas melhores práticas de segurança reconhecidas.

- As medidas de segurança impostas aos OSEs não devem, em qualquer caso, exigir que produtos específicos das TIC sejam concebidos, desenvolvidos ou fabricados de forma específica (Considerando 51).

## b) Aplicação alargada da comunicação de incidentes de segurança

- Os operadores de serviços essenciais estão obrigados a comunicar os incidentes de segurança nos seus PSDs contratados que tenham impacto na continuidade dos seus serviços essenciais (Artigo 16.5). Assim sendo, os PSDs terão, no âmbito do contrato, de reportar a esse operador essencial os incidentes de segurança que possam ter impacto nos mesmos.

- Agradecemos a flexibilidade quanto ao prazo de notificação dos OSEs inerente à expressão "sem demora indevida" (Artigo 14.3). As transposições nacionais não devem introduzir prazos específicos e, em qualquer caso, caso seja pedido aos OSEs que justifiquem o tempo necessário para a notificação, o período em relação ao qual são julgados deve ter início quando os OSEs estão cientes do incidente, não a partir de quando os PSDs estão cientes do mesmo.

- O Artigo 14.7 prevê que o Grupo de Cooperação elabore diretrizes sobre as circunstâncias para a notificação, em oposição ao papel de harmonização da Comissão relativamente às notificações dos PSDs. Dada a exigência de duplicação de relatórios relativamente aos PSDs, é importante que os respetivos requisitos de notificação não sejam contraditórios e estejam o mais alinhados possível. Assim sendo, este processo deve ser analisado tendo em mente esse objetivo. Além disso, os requisitos de notificação para os PSDs devem respeitar as obrigações de confidencialidade que têm para com os seus clientes OSEs, não lhes pedindo para partilhar informações comerciais confidenciais.

# ACERCA DA DIGITALEUROPE

A DIGITALEUROPE representa a indústria de tecnologia digital na Europa. Os nossos membros incluem algumas das maiores empresas mundiais de TI, telecomunicações e eletrónica de consumo, bem como associações nacionais de toda a Europa. A DIGITALEUROPE pretende que as empresas e os cidadãos europeus possam beneficiar plenamente das tecnologias digitais e que a Europa desenvolva, atraia e mantenha as melhores empresas de tecnologia digital do mundo.

A DIGITALEUROPE garante a participação da indústria no desenvolvimento e implementação das políticas da UE. Os membros da DIGITALEUROPE incluem 62 membros corporativos e 37 associações comerciais nacionais de toda a Europa. O nosso site fornece mais informações sobre as nossas notícias e atividades recentes: http://www.digitaleurope.org

# FILIAÇÃO DIGITALEUROPE

## Membros corporativos

Airbus, Amazon Web Services, AMD, Apple, BlackBerry, Bose, Brother, CA Technologies, Canon, Cisco, Dell, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Ingram Micro, Intel, iQor, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Samsung, SAP, SAS, Schneider Electric IT Corporation, Sharp Electronics, Siemens, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, Zebra Technologies, ZTE Corporation.

## Associações nacionais de comércio

**Alemanha:** BITKOM, ZVEI
**Áustria:** IOÖ
**Bélgica:** AGORIA
**Bielorrússia:** INFOPARK
**Bulgária:** BAIT
**Chipre:** CITEA
**Dinamarca:** DI Digital, IT-BRANCHEN
**Eslováquia:** ITAS
**Eslovénia:** GZS
**Espanha:** AMETIC
**Estónia:** ITL
**Finlândia:** FFTI
**França:** AFNUM, Force Numérique, Tech in France
**Grécia:** SEPE
**Holanda:** Nederland ICT, FIAR
**Hungria:** IVSZ
**Irlanda:** ICT IRELAND
**Itália:** ANITEC
**Lituânia:** INFOBALT
**Polónia:** KIGEIT, PIIT, ZIPSEE
**Portugal:** AGEFE
**Reino Unido:** techUK
**Roménia:** ANIS, APDETIC
**Suécia:** Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
**Suíça:** SWICO
**Turquia:** Digital Turkey Platform, ECID
**Ucrânia:** IT UKRAINE