PRESIDÊNCIA DO CONSELHO DE MINISTROS
Gabinete Nacional de Segurança

Para:
ANACOM – Autoridade Nacional de Comunicações
Av. José Malhoa, 12
1099-017 Lisboa

Ofício GNS/CNCS Data: 03OUT2018

Assunto: **CONTRIBUTO NO ÂMBITO DO PROCEDIMENTO DE ELABORAÇÃO DE UM REGULAMENTO RELATIVO À SEGURANÇA E À INTEGRIDADE DAS REDES E SERVIÇOS DE COMUNICAÇÕES ELETRÓNICAS**

Junto se envia o contributo do Gabinete Nacional de Segurança/Centro Nacional Cibersegurança no âmbito do procedimento de elaboração de um regulamento relativo à segurança e integridade das redes e serviços de comunicações eletrónicas.

Com os melhores cumprimentos,

O DIRETOR-GERAL

António Gameiro Marques

CALM

Em anexo: Contributo do GNS/CNCS.

ANEXO

Assunto: **CONTRIBUTO DO GABINETE NACIONAL DE SEGURANÇA/CENTRO NACIONAL DE CIBERSEGURANÇA NO ÂMBITO DO PROCEDIMENTO DE ELABORAÇÃO DE UM REGULAMENTO RELATIVO À SEGURANÇA E À INTEGRIDADE DAS REDES E SERVIÇOS DE COMUNICAÇÕES ELETRÓNICAS**

1. Sem prejuízo dos contributos a seguir explanados, o Gabinete Nacional de Segurança (GNS)/Centro Nacional Cibersegurança (CNCS) vem, nos termos do n.º 1 do artigo 98.º do Código do Procedimento Administrativo e dos n.ºs 10 e 11 da nota justificativa do Aviso n.º 11948/2018, publicado no Diário da República, 2.ª série, n.º 161, de 22 de agosto de 2018, informar que se pretende constituir como interessado no âmbito do procedimento de elaboração de um regulamento relativo à segurança e integridade das redes e serviços de comunicações eletrónicas.

2. O GNS/CNCS congratula-se com a iniciativa da ANACOM – Autoridade Nacional de Comunicações (ANACOM) de consulta no âmbito do procedimento de elaboração deste regulamento.

3. Nos termos dos n.ºs 1 e 2 da Lei n.º 46/2018, de 13 de agosto, o CNCS funciona no âmbito do GNS e é a Autoridade Nacional de Cibersegurança, tendo por missão garantir que o País usa o ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes, bem como da definição e implementação das medidas e instrumentos necessários à antecipação, deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes, ponham em causa o interesse nacional, o funcionamento da Administração Pública, dos operadores de infraestruturas críticas, dos operadores de serviços essenciais e dos prestadores de serviços digitais.

4. Foi atribuída ao GNS / CNCS a competência, em razão da matéria, para proceder à transposição da Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União (Diretiva SRI), tendo sido para este efeito aprovada *supra*referida Lei n.º 46/2018 de 13 de agosto, que estabelece o regime jurídico da segurança do ciberespaço.

5. A Lei das Comunicações Eletrónicas (LCE), aprovada pela Lei n.º 5/2004, de 10 de fevereiro, na sua redação atual, tem um âmbito de aplicação específico pelo que se entende que o regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas deverá respeitar essa premissa de forma compatível com a Lei n.º 46/2018 de 13 de agosto, não devendo extrapolar através da previsão legal a matéria que se pretende regulamentar.

6. Assim, com o objetivo da participação e contributo do GNS/CNCS nos termos indicados no n.º 1, cabe em seguida a análise do Projeto de Regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas, aprovado pela ANACOM em 6 de julho de 2018, publicado no Aviso n.º 11948/2018 [1], considerando para este efeito o disposto na LCE, na 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 dos sistemas de informação em toda a União [2] e na Lei n.º 46/2018, de 13 de agosto, que estabelece o regime jurídico da segurança do ciberespaço.

[1] A seguir referenciado como Projeto de Regulamento.
[2] A seguir referenciada como Diretiva SRI.

I – A Diretiva SRI e a Lei n.º 46/2018, de 13 de agosto

Importa expor previamente os seguintes preceitos da Diretiva SRI e da Lei n.º 46/2018, de 13 de agosto, para posterior apreciação do âmbito de aplicação do Projeto de Regulamento da ANACOM.

7. A Diretiva SRI estabelece medidas destinadas a alcançar um elevado nível comum de segurança das redes e dos sistemas de informação na União, a fim de melhorar o funcionamento do mercado interno, e para este efeito estabelece requisitos de segurança e de notificação de incidentes para os operadores de serviços essenciais e para os prestadores de serviços digitais, cf. o n.º 1 e alínea d) do n.º 2 do artigo 1.º da Diretiva SRI, com a epígrafe "Objeto e âmbito de aplicação".

8. Dispõe o 7.º parágrafo dos considerandos da Diretiva SRI que " (…) as obrigações que recaem sobre os operadores de serviços essenciais e sobre os prestadores de serviços digitais não deverão aplicar-se às empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público, na aceção da Diretiva 2002/21/CE do Parlamento Europeu e do Conselho , que estão sujeitas aos requisitos específicos de segurança e integridade estabelecidos na referida diretiva" .

9. Neste sentido prevê o n.º 3 do *supra*referido artigo 1.º da Diretiva SRI, que "Os requisitos de segurança e de notificação previstos na presente diretiva não se aplicam às empresas sujeitas aos requisitos previstos nos artigos 13.º-A e 13.º-B da Diretiva 2002/21/CE".

10. O Anexo II da Diretiva SRI identifica a tipologia de operadores de serviços essenciais, incluindo-se um setor das infraestruturas digitais com os seguintes tipos de entidades: pontos de troca de tráfego; prestadores de serviços de DNS; registos de nomes de domínio de topo.

11. O Anexo III da Diretiva SRI identifica a seguinte tipologia de serviços digitais: mercados em linha; motores de pesquisa em linha; serviços de computação em nuvem.

12. De acordo com o exposto prevê a Lei n.º 46/2018, de 13 de agosto respetivamente nos artigos 16.º e 17.º requisitos de segurança e requisitos de notificação de incidentes a aplicar por operadores de serviços essenciais.

13. O Anexo da Lei n.º 46/2018, de 13 de agosto identifica a tipologia de operadores de serviços essenciais, incluindo-se um setor das infraestruturas digitais com os seguintes tipos de entidades: pontos de troca de tráfego; prestadores de serviços de DNS; registos de nomes de domínio de topo.

14. O artigo 11.º da Lei n.º 46/2018, de 13 de agosto prevê que os prestadores de serviços digitais prestam os seguintes serviços: serviço de mercado em linha; serviço de motor de pesquisa em linha; serviço de computação em nuvem.

II – O Projeto de Regulamento da ANACOM

15. O Projeto de Regulamento da ANACOM prevê no artigo 1.º o respetivo objeto a seguir elencado, remetendo para o enquadramento legal da LCE [3], a qual consubstancia a transposição, da, entre outras, a Diretiva 2002/21/CE do Parlamento Europeu e do Conselho de 7 de março de 2002 relativa a um quadro regulamentar comum para as redes e serviços de comunicações eletrónicas, com as alterações da Diretiva 2009/140/CE, do Parlamento Europeu e do Conselho, de 25 de novembro de 2009 [4], com a introdução da

[3] Lei n.º 5/2004, de 10 de fevereiro, republicada pela Lei n.º 51/2011, de 13 de setembro, e alterada pela Lei n.º 10/2013, de 28 de janeiro, pela Lei n.º 42/2013, de 3 de julho, pelo Decreto-Lei n.º 35/2014, de 7 de março, pela Lei n.º 82-B/2014, de 31 de dezembro, pela Lei n.º 127/2015, de 3 de setembro, pela Lei n.º 15/2016, de 17 de junho, e pelo Decreto-Lei n.º 92/2017, de 31 de julho.

[4] A LCE realiza o processo de transposição das Diretivas n.º 2002/19/CE, 2002/20/CE e 2002/21/CE, todas do Parlamento Europeu e do Conselho, de 7 de março, alteradas pela Diretiva n.º 2009/140/CE, do Parlamento Europeu e do Conselho, de 25 de novembro, e das Diretivas n.º 2002/22/CE, do Parlamento Europeu e do Conselho, de 7 de março, alterada pela Diretiva n.º 2009/136/CE, do Parlamento Europeu e do Conselho, de 25 de novembro, e da Diretiva 2002/77/CE, da Comissão Europeia, de 16 de setembro, cf. artigo 1.º da LCE.

previsão da regulamentação da matéria da segurança e integridade das redes e serviços indicando que o Projeto de Regulamento estabelece:

i. As medidas técnicas de execução e os requisitos adicionais a cumprir pelas empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público em matéria de segurança e integridade para os efeitos do disposto no artigo 54.º-A e nos termos previstos no n.º 1 do artigo 54.º-C e no artigo 54.º-D da LCE.

ii. As circunstâncias, o formato e os procedimentos aplicáveis às exigências de comunicação de violações de segurança ou perdas de integridade das redes com impacto significativo no funcionamento das redes e serviços pelas empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público, ao abrigo do disposto no artigo 54.º-B e no n.º 2 do artigo 54.º-C da LCE.

iii. As condições em que as empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público devem divulgar ao público as violações de segurança ou as perdas de integridade com impacto significativo no funcionamento das redes e serviços, ao abrigo do disposto na alínea b) do artigo 54.º-E da LCE.

iv. As obrigações de realização de auditorias à segurança das redes e serviços e de envio do respetivo relatório pelas empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público, bem como os requisitos a que devem obedecer as auditorias e os requisitos aplicáveis às entidades auditoras, ao abrigo do disposto nos n.ºs 1 e 2 do artigo 54.º-F da LCE.

III – A aplicação do Projeto de Regulamento da ANACOM

16. O Projeto de Regulamento delimita o respetivo âmbito de aplicação em concreto através de definições previstas no respetivo artigo 3.º, referindo-se as seguintes:

i. "Ativos", as infraestruturas, os sistemas de transmissão ou de informação, os equipamentos e os demais recursos, físicos e lógicos, que compõem ou suportam uma rede de comunicações públicas e respetivos acessos, **incluindo interligações**, um serviço de comunicações eletrónicas acessível ao público ou **um serviço conexo associado"** cf. a alínea a) do artigo 3.º do Projeto de Regulamento.

ii. "Segurança das redes e serviços", a capacidade das redes ou dos serviços de comunicações eletrónicas para resistir, com um dado nível de confiança, a qualquer ação que comprometa a disponibilidade, a autenticidade, a integridade ou a confidencialidade dessas redes e serviços, dos dados armazenados, transmitidos ou tratados ou dos **serviços associados oferecidos ou acessíveis através dessas redes ou serviços"** cf. a alínea m) do artigo 3.º do Projeto de Regulamento.

17. Cumpre enunciar a possível inclusão de operadores de serviços essenciais referentes à tipologia de infraestruturas digitais e de prestadores de serviços digitais, nas definições referentes a "Ativos" e a "Segurança das redes e serviço" através da utilização das expressões:

i. "incluindo interligações", em correspondência técnica a qualquer interligação incluindo "pontos de troca de tráfego". Permanece a dúvida ainda que se remeta para a definição de "Interligação" tal como consta da alínea o) do artigo 3.º da LCE: "Interligação: a ligação física e lógica de redes de comunicações públicas utilizadas por uma mesma empresa ou por empresas diferentes de modo a permitir a utilizadores de uma empresa comunicarem com utilizadores desta ou

de outras empresas ou acederem a serviços oferecidos por outra empresa. Os serviços podem ser oferecidos pelas partes envolvidas ou por terceiros que tenham acesso à rede. A interligação é um tipo específico de acesso implementado entre operadores de redes públicas".

ii. "um serviço conexo associado", com possível correspondência técnica a qualquer serviço conexo associado incluindo "pontos de troca de tráfego", "prestadores de serviços de DNS"; "registos de nomes de domínio de topo". Permanece a dúvida ainda que se remeta para a definição de "Serviços conexos" tal como consta da alínea gg) do artigo 3.º da LCE: "Serviços conexos, os serviços associados a uma rede de comunicações eletrónicas e ou a um serviço de comunicações eletrónicas que permitem e ou servem de suporte à oferta de serviços através dessa rede e ou serviço, ou têm potencial para fazê-lo, e incluem nomeadamente os sistemas de conversão de números ou os sistemas que oferecem uma funcionalidade equivalente, os sistemas de acesso condicional e os guias eletrónicos de programas, bem como outros serviços como o serviço de identidade, localização e presença".

iii. "serviços associados oferecidos ou acessíveis através das redes ou serviços", com possível correspondência técnica a quaisquer serviços associados oferecidos ou acessíveis através das redes ou servições incluindo "pontos de troca de tráfego", "prestadores de serviços de DNS"; "registos de nomes de domínio de topo" bem como (pela expressão "acessíveis através") a prestadores de serviços digitais previstos nos n.ºs 5 e 6 e Anexo III da Diretiva SRI e no artigo 11.º da Lei n.º 46/2018, de 13 de agosto "mercados em linha"; "motores de pesquisa em linha"; "serviços de computação em nuvem".

18. Quanto ao Projeto de Regulamento deverão ainda ser especialmente considerados os seguintes pontos que concretizam a execução e aplicação prática deste diploma aos objetos *supra* indicados:

— Âmbito (artigo 2.º).

- Cooperação e partilha de informação (artigo 4.º).
- Obrigações das empresas em matéria de segurança e integridade (Título II).
- Obrigações de notificação e de informação ao público (Título III).
- Auditorias à segurança das redes e serviços (Título IV)
- Regime sancionatório (artigo 34.º).

19. Face ao exposto, em virtude de o âmbito do Projeto de Regulamento ser delimitado por definições que poderão corresponder à tipologia de infraestruturas digitais (operadores de serviços essenciais) e de prestadores de serviços digitais tal como previstos na Diretiva SRI e na Lei n.º 46/2018, de 13 de agosto, torna-se patente que a interpretação e aplicação deste Regulamento poderá conflituar com o cabal cumprimento do regime jurídico da segurança do ciberespaço definido na Lei n.º 46/2018, de 13 de agosto e que, por isso, deverá no Projeto de Regulamento da ANACOM ser incluída cláusula de salvaguarda do domínio da Autoridade Nacional de Cibersegurança em referência à Lei n.º 46/2018, de 13 de agosto e a regulamentação decorrente.

IV – Conclusões

20. Considerando que:

- A execução do Projeto de Regulamento da ANACOM em análise é realizada em cumprimento dos artigos a seguir transcritos da LCE:

Artigo 54.º-A Obrigações das empresas em matéria de segurança e integridade

1 - As empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público devem adotar as medidas técnicas e organizacionais adequadas à prevenção, gestão e redução dos riscos para a segurança das redes e serviços visando, em especial, impedir ou

minimizar o impacte dos incidentes de segurança nas redes interligadas, a nível nacional e internacional, e nos utilizadores.
2 - As empresas que oferecem redes de comunicações públicas são obrigadas a adotar as medidas adequadas para garantir a integridade das respetivas redes, assegurando a continuidade da prestação dos serviços que se suportam nas referidas redes.
3 - As medidas previstas no n.º 1 devem ser adequadas aos riscos existentes tendo em conta o estado da técnica.

Artigo 54.º-B Obrigações de notificação
As empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público estão obrigadas a notificar a ARN das violações de segurança ou das perdas de integridade com impacte significativo no funcionamento das redes e serviços.

- A LCE prevê no n.º 3 do seu artigo 2.º que em caso de conflito entre normas da LCE e as normas estabelecidas na restante legislação sectorial aplicável, prevalecem as normas da LCE salvo quando de outra disposição resulte um regime mais exigente para as empresas que oferecem redes e serviços de comunicações eletrónicas, caso em que será este o aplicável.
- O n.º 7 das referências introdutórias da Diretiva SRI prevê que as obrigações que recaem sobre os operadores de serviços essenciais e sobre os prestadores de serviços digitais não deverão aplicar-se às empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público, na aceção da Diretiva 2002/21/CE do Parlamento Europeu e do Conselho, que estão sujeitas aos requisitos específicos de segurança e integridade estabelecidos na Diretiva 2002/21/CE. No mesmo sentido dispõe o n.º 3 do artigo 3.º da Diretiva SRI, determinando que os requisitos de segurança e de notificação previstos na Diretiva SRI não se aplicam às empresas sujeitas aos requisitos previstos nos artigos 13.º-A e 13.º-B da Diretiva 2002/21/CE.

— De acordo a Lei n.º 46/2018, de 13 de agosto prevê, respetivamente, na alínea a) do seu artigo 12.º e na alínea a) do n.º 2 do artigo 13.º, que os requisitos de segurança e de notificação de incidentes não se aplicam às empresas sujeitas aos requisitos previstos nos artigos 54.º-A a 54.º-G da lei das comunicações eletrónicas, aprovada pela Lei n.º 5/2004, de 10 de fevereiro, na sua redação atual.

— O âmbito de aplicação do Projeto de Regulamento da ANACOM é delimitado por definições que poderão corresponder à tipologia de infraestruturas digitais (operadores de serviços essenciais) e de prestadores de serviços digitais tal como previstos na Diretiva SRI e na Lei n.º 46/2018, de 13 de agosto, tornando-se patente que a interpretação e aplicação deste Regulamento poderá conflituar com o cabal cumprimento do regime jurídico da segurança do ciberespaço definido na Lei n.º 46/2018, de 13 de agosto.

21. Conclui-se com a seguinte proposta:

Em virtude de o atual âmbito de aplicação em concreto pretendido do Projeto de Regulamento da ANACOM permitir sobreposição de competências na aplicação do normativo de regulamentação da LCE com a Lei n.º 46/2018, de 13 de agosto, pelas respetivas autoridades nacionais competentes propõe-se que seja incluída no Projeto de Regulamento da ANACOM cláusula de salvaguarda do domínio de competências da Autoridade Nacional de Cibersegurança em referência à Lei n.º 46/2018, de 13 de agosto e a regulamentação decorrente nos termos que se enunciam:

— *O disposto no presente Regulamento não prejudica o cumprimento do regime jurídico da segurança do ciberespaço designadamente da Lei n.º 46/2018, de 13 de agosto e respetiva regulamentação, no quadro de competências da Autoridade Nacional de Cibersegurança.*

Em conformidade com o exposto propõe-se ainda que:

- No artigo 15.º do Projeto de Regulamento da ANACOM seja adicionado o dever de colaboração mútua entre a ANACOM e o CNCS, para as alíneas a), b), c), d), f) e g).
- Da constituição das equipas referidas no artigo 16.º do Projeto de Regulamento da ANACOM seja dado conhecimento ao CNCS, por assegurar o serviço de CSIRT Nacional.
- Na alínea a) do artigo 20.º do Projeto de Regulamento da ANACOM seja realizada referência ao CNCS e à Lei n.º 46/2018, de 13 de agosto.
- No artigo 21.º do Projeto de Regulamento da ANACOM seja previsto que o CNCS seja informado quando o impacto de um incidente afete setores ou entidades no âmbito de aplicação da Lei n.º 46/2018, de 13 de agosto ou quando este impacto seja transfronteiriço em virtude das competências do CNCS.
- Em conformidade com o exposto no nº 1 do artigo 22.º do Projeto de Regulamento da ANACOM substituir "ao abrigo do disposto no número anterior" por "ao abrigo do disposto nos artigos anteriores", considerando que se propõe a realização de notificação também ao CNCS na alínea a) do artigo 20.º do Projeto de Regulamento da ANACOM.
- Seja incluída referência à ANACOM como ponto de contacto setorial responsável pela comunicação com as restantes autoridades e entidades nacionais com responsabilidades pela segurança das redes e dos sistemas de informação, como é o caso do CNCS, enquanto Autoridade Nacional de Cibersegurança, quando um incidente de segurança produza um impacto ou tenha o potencial para tal, em outros setores e entidades.
- O n.º 15 do artigo 22.º do Projeto de Regulamento da ANACOM se abranja na cooperação, para além das entidades impactadas, as autoridades e entidades nacionais com especial responsabilidade no ecossistema da segurança das redes e sistemas de informação como o CNCS, para a correta

deteção e avaliação de impacto de violação de segurança ou perda de integridade e a respetiva notificação.

22. Neste sentido solicita-se que sejam salvaguardadas as recomendações efetuadas no presente documento.

23. Assim, afigura-se essencial uma estreita cooperação as autoridades nacionais relevantes neste domínio, por forma a permitir criar um quadro jurídico claro e que permita soluções dotadas de certeza e segurança jurídica. Neste sentido, quer o processo de elaboração deste regulamento, quer o processo de regulamentação da Lei n.º 46/2018, de 13 de agosto constituem oportunidades para atingir este desiderato.

Lisboa, 03 de outubro de 2018.