Projeto de regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas

Relatório da consulta pública

Julho de 2018

Índice

1. Enquadramento 3

2. Comentários gerais 6

3. Propostas apresentadas 13

4. Comentários específicos 17

4.1. Título I 17

4.2. Título II 21

4.3. Título III 29

4.4. Título IV 34

4.5. Título V 38

5. Conclusão 40

1. Enquadramento

Por decisão de 4 de agosto de 2016 e ao abrigo do disposto nos seus Estatutos ([1]) e na Lei das Comunicações Eletrónicas ([2]), a Autoridade Nacional de Comunicações (ANACOM) aprovou o início do procedimento de elaboração de um regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas, bem como a publicitação do respetivo anúncio, nos termos previstos no n.º 1 do artigo 98.º do Código do Procedimento Administrativo ([3]).

Na sequência desse anúncio, foram submetidos os seguintes 18 contributos iniciais:

- ANPC – Autoridade Nacional de Proteção Civil;
- Associação para a Promoção e Desenvolvimento da Sociedade de Informação (APDSI);
- Banco de Portugal;
- Cabovisão – Televisão por Cabo, S.A. e ONITELECOM Infocomunicações, S.A.;
- DGAE – Direção-Geral das Atividades Económicas;
- DGEG – Direção-Geral de Energia e Geologia;
- EDP Distribuição – Energia, S.A.;
- ERSE – Entidade Reguladora dos Serviços Energéticos;
- Entidade de Serviços Partilhados da Administração Pública, I.P. (eSPap);
- FCT – Fundação para a Ciência e a Tecnologia;
- Gabinete Nacional de Segurança/Centro Nacional Cibersegurança;
- Guarda Nacional Republicana;

([1]) Aprovados em anexo ao Decreto-Lei n.º 39/2015, de 16 de março.

([2]) 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.

([3]) Aprovado em anexo ao Decreto-Lei n.º 4/2015, de 7 de janeiro.

- Governo Regional da Região Autónoma dos Açores;
- Instituto Nacional de Emergência Médica, I.P.;
- Secretaria Geral do Ministério da Administração Interna;
- NOS Comunicações, S.A., NOS Açores Comunicações, S.A. e NOS Madeira Comunicações, S.A.;
- Polícia Judiciária; e
- Governo Regional da Região Autónoma da Madeira.

Analisados os contributos iniciais recebidos, a ANACOM aprovou, por decisão de 29 de dezembro de 2016, o projeto de regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas («**Projeto**»), o qual foi submetido ao adequado procedimento regulamentar e procedimento geral de consulta pelo período de 30 dias úteis ([4]), nos termos previstos no artigo 10.º dos Estatutos da ANACOM e dos artigos 98.º e seguintes do Código do Procedimento Administrativo e para os efeitos previstos no artigo 8.º e, em especial, no n.º 4 do artigo 54.º-C da Lei das Comunicações Eletrónicas.

Após prorrogação do prazo em 15 dias úteis ([5]), a consulta pública decorreu até ao dia 14 de março de 2017, tendo sido oportunamente recebidas as seguintes 17 pronúncias:

- APRITEL – Associação dos Operadores de Comunicações Eletrónicas («**APRITEL**»);
- DECO – Associação Portuguesa para a Defesa do Consumidor («**DECO**»);
- Comissão Técnica 80 – Gestão da Qualidade e Garantia da Qualidade («**CT 80**»);
- Comissão Técnica 163 – Segurança em Sistemas de Informação («**CT 163**»);
- DELOITTE & Associados, S.R.O.C., S.A. («**DELOITTE**»);
- EDP Distribuição – Energia, S.A. («**EDP**»);
- Estado-Maior-General das Forças Armadas («**EMGFA**»);
- FCT – Fundação para a Ciência e a Tecnologia («**FCT**»);
- Gabinete Nacional de Segurança/Centro Nacional de Cibersegurança («**GNS/CNCS**»);

([4]) Através do Aviso n.º 459/2017, publicado a 10 de janeiro na 2.ª Série (Parte E) do Diário da República.

([5]) Através do Aviso n.º 2054/2017, publicado a 23 de fevereiro na 2.ª Série (Parte E) do Diário da República.

- MEO – Serviços de Comunicações e Multimédia, S.A. («**MEO**»);
- NOS Comunicações, S.A., NOS Açores Comunicações, S.A. e NOS Madeira Comunicações, S.A. («**GRUPO NOS**»);
- NOWO Communications, S.A. e ONITELECOM Infocomunicações, S.A. («**NOWO/ONITELECOM**»);
- Procuradoria-Geral da República («**PGR**»);
- RENTELECOM Comunicações, S.A. («**RENTELECOM**»);
- Secretaria Geral do Ministério da Administração Interna («**SGMAI**»);
- Serviço Regional de Proteção Civil e Bombeiros dos Açores («**SRPCBA**»); e
- Vodafone Portugal, Comunicações Pessoais, S.A. («**VODAFONE**»).

O presente relatório contém referência às pronúncias recebidas e a apreciação global da ANACOM, que reflete o seu entendimento sobre as mesmas e que fundamenta as opções que levam a ANACOM a adotar um segundo projeto relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas («**2.º Projeto**»), a submeter a novo procedimento regulamentar e procedimento geral de consulta, em cumprimento do disposto no artigo 10.º dos Estatutos da ANACOM, nos artigos 98.º e seguintes do Código do Procedimento Administrativo e para os efeitos previstos no artigo 8.º e, em especial, no n.º 4 do artigo 54.º-C da Lei das Comunicações Eletrónicas.

As pronúncias integrais, na sua versão não confidencial, quando seja o caso, são disponibilizadas no sítio institucional da ANACOM na Internet, em www.anacom.pt, em conjunto com o presente relatório.

A leitura do presente relatório e, em particular, das referências às alterações a introduzir no 2.º Projeto – que não são exaustivas, limitando-se às alterações mais significativas, que se entendeu dever salientar –, não prejudica, nem substitui, uma análise do mesmo.

2. Comentários gerais

No essencial, foram apresentados, entre outros ([6]), os seguintes **comentários gerais**:

(1) No que respeita à **<u>fundamentação</u>**, que o Projeto não se encontrava devidamente fundamentado, nomeadamente por não se demonstrar o seu suporte:

a) Numa análise de custos e benefícios e numa avaliação do respetivo impacto, considerando as medidas já adotadas pelas empresas, os riscos e as ameaças no contexto nacional e o atual contexto económico e financeiro (**APRITEL, pág. 3**; **MEO, pág. 4**; **GRUPO NOS, págs. 3 e 10 a 12**; **NOWO/ONITELECOM, págs. 2, 4 e 7**; **VODAFONE, págs. 3 e 4**); e

b) Num exercício de *benchmarking*, não tendo em consideração as medidas adotadas por outros Estados-Membros e revelando-se como a solução mais exigente de entre várias soluções analisadas, sem que os riscos e as ameaças no contexto nacional o justifiquem (**APRITEL, págs. 3 e 5**; **GRUPO NOS, págs. 3 e 6 a 8**; **NOWO/ONITELECOM, págs. 2 e 7**; **VODAFONE, pág. 5**);

<u>Entendimento da ANACOM</u>

Em **2010**, a ANACOM realizou um **estudo de avaliação e caracterização da segurança em redes de comunicações públicas**, o qual se focou numa análise da infraestrutura e dos recursos de uma amostra representativa de operadores de rede e de prestadores de serviços nacionais, bem como das políticas, medidas, práticas, planos, meios e recursos por eles afetos à segurança de redes e de informação.

([6]) Ver, nomeadamente, APRITEL, págs. 1 a 7, CT 80, CT 163, ponto 1, DECO, ponto I, DELOITTE, ponto I, EDP, págs. 1 a 3, EMGFA, pontos 1 a 4, FCT, GNS/CNCS, GRUPO NOS págs. 3 a 14, MEO, págs. 3 a 9, NOWO/ONITELECOM, págs. 1 a 7, PGR, RENTELECOM, SGMAI, SRPCBA e VODAFONE, págs. 1 a 8.

Neste estudo, foram ainda identificados e caracterizados os principais tipos de interdependências entre as diferentes redes e serviços de comunicações eletrónicas, bem como avaliado e caracterizado o risco associado à situação encontrada, em termos das principais vulnerabilidades identificadas e de alguns cenários de ameaças.

Do estudo resultou um conjunto de recomendações, destinadas aos diversos intervenientes, públicos e privados, de forma a fortalecer a robustez e disponibilidade das redes de comunicações públicas e dos serviços de comunicações eletrónicas acessíveis ao público, sendo, em termos temporais, considerada uma perspetiva de futuro de curto e médio prazo.

Dois anos mais tarde, em **2012**, procedeu esta Autoridade a uma **avaliação da segurança e integridade das redes e serviços de comunicações eletrónicas a nível nacional**, a qual se baseou, então, no documento da ENISA – *European Union Agency for Network and Information Security* («**ENISA**») "*Technical Guideline for Minimum Security Measures: Guidance on the security measures in Article 13a (Version 1.0, December 2011)"*.

Para o efeito, foi solicitado, através de ofício dirigido a todas as empresas que oferecem redes de comunicações públicas e/ou serviços de comunicações eletrónicas acessíveis ao público, a indicação do estado de implementação, para cada medida presente em cada um dos subdomínios, dos domínios D1 a D7, constantes do Capítulo 3 ("*Minimum Security Measures*") do referido documento da ENISA.

A informação recolhida contribuiu para determinar a situação existente ao nível das empresas que oferecem redes de comunicações públicas e/ou serviços de comunicações eletrónicas acessíveis ao público face ao referencial europeu publicado pela ENISA e foi utilizada pela ANACOM para o desenvolvimento do Projeto e, agora, do 2.º Projeto.

Em particular para a elaboração e revisão do Título III, mas também para a elaboração e revisão dos demais títulos, contribuiu também a informação e a

experiência recolhida pela ANACOM desde **2014**, através do respetivo **centro de reporte**, no tratamento das notificações recebidas, no acompanhamento das violações de segurança ou perdas de integridade em causa e no âmbito da sua análise agregada.

Mais recentemente, é ainda de salientar a informação e a experiência recolhida através do acompanhamento, pela ANACOM, do impacto nas redes de comunicações públicas e nos serviços de comunicações eletrónicas acessíveis ao público dos **incêndios ocorridos em 17 de junho** e em **15 de outubro de 2017**, através:

a) Quer de um esforço de levantamento desse impacto, incluindo um *site survey*;

b) Quer da coordenação de um grupo de trabalho, constituído por entidades públicas e privadas, designadamente a Associação Empresarial de Comunicações de Portugal (ACIST), a Autoridade Nacional de Proteção Civil (ANPC), a APRITEL, a Direção-Geral de Energia e Geologia (DGEG), a Entidade Reguladora dos Serviços Energéticos (ERSE), o Instituto de Telecomunicações e empresas dos setores das comunicações eletrónicas, dos transportes e da energia.

Da missão deste grupo de trabalho acabou por resultar a elaboração do "*Relatório do Grupo de Trabalho dos Incêndios Florestais – Medidas de Proteção e Resiliência de Infraestruturas de Comunicações Eletrónicas*", disponível no sítio institucional da ANACOM na Internet, apresentado publicamente em sessão promovida pela ANACOM a 29.05.2018, com 27 medidas que permitirão reduzir significativamente o impacto dos incêndios florestais nas redes e serviços de comunicações eletrónicas e, consequentemente, nos seus utilizadores.

As lições retiradas desta experiência, até ao momento, foram devidamente consideradas na elaboração do 2.º Projeto, salientando-se, em particular e entre outras disposições, os novos n.os 2 e 3 do artigo 2.º, o novo n.º 3 do artigo 6.º, as alterações introduzidas no conteúdo das notificações de violações de segurança ou

perdas de integridade com impacto significativo, no âmbito do artigo 22.º, e, em geral, as disposições relevantes constantes do novo Anexo.

Por último e no que respeita à questão do *benchmarking*, a revisão do Título II do projeto de regulamento tendo agora por base, com as devidas adaptações, o documento da ENISA "*Technical Guideline on Security Measures (Technical guidance on the security measures in Article 13a) – Version 2.0, October 2014*" («***Technical Guideline on Security Measures***»), disponível em www.enisa.europa.eu, nos termos previstos nos artigos 6.º e 7.º e no Anexo do 2.º Projeto e abaixo expostos e fundamentados, permite não só responder favoravelmente a muitos dos contributos recebidos, como também promover uma maior harmonização com os demais Estados-Membros da União Europeia.

(2) No que respeita à **proporcionalidade**, que as medidas impostas não são proporcionais, nomeadamente por não serem adequadas aos riscos e às ameaças no contexto nacional e ao contexto específico de cada empresa, atenta a sua natureza prescritiva e pouco flexível, implicando um impacto muito significativo e não promovendo um investimento eficiente (**APRITEL, págs. 1 a 5**; **MEO, págs. 4 e 8**; **GRUPO NOS, pág. 9**; **NOWO/ONITELECOM, págs. 2, 4 e 7**; **RENTELECOM, pág. 2**; **VODAFONE, págs. 2 e 4**);

Entendimento da ANACOM

Sobre esta matéria e considerando ser a mesma essencial na fundamentação da nova abordagem adotada no âmbito do 2.º Projeto, remetemos para o entendimento da ANACOM no *ponto (2)* em *3. Propostas apresentadas*, abaixo.

(3) No que respeita à **legalidade**, que as medidas impostas, ao corresponderem a um nível de exigência acima do *standard* da indústria, não se encontram conformes com o disposto no n.º 3 do artigo 54.º-C da Lei das Comunicações Eletrónicas, nos termos do qual (com sublinhados nossos) "*as medidas de execução (…) devem ser conformes com as decisões da Comissão Europeia adotadas ao abrigo do procedimento previsto no artigo 13.º-A da Diretiva n.º 2002/21/CE, do Parlamento Europeu e do Conselho, de 7 de Março, alterada pela Diretiva n.º 2009/140/CE, do*

Parlamento Europeu e do Conselho, de 25 de Novembro, e, na sua ausência, <u>devem basear-se nas normas europeias e internacionais existentes sobre a matéria</u>" (**VODAFONE, pág. 4**);

<u>Entendimento da ANACOM</u>

Nos termos previstos no n.º 3 do artigo 54.º-C da Lei das Comunicações Eletrónicas, as medidas a aprovar pela ANACOM ao abrigo do disposto no n.º 1 do mesmo artigo devem, na ausência de decisões da Comissão Europeia, basear-se nas normas europeias e internacionais existentes sobre a matéria, mas não se encontram limitadas às mesmas – nem poderia ser esse o caso, atendendo à necessária adequação dessas medidas aos riscos existentes, tendo em conta o estado da técnica, nos termos explicitamente previstos no n.º 3 do artigo 54.º-A do mesmo diploma.

Em qualquer caso, sempre se adianta que no 2.º Projeto se acaba por preconizar, como regra geral – com as devidas exceções – e nos termos previstos nos respetivos artigos 6.º e 7.º, o nível de sofisticação 2 (*norma de indústria*). Sobre esta nova abordagem, remetemos, também aqui, para o entendimento da ANACOM no *ponto (2)* em *3. Propostas apresentadas*, abaixo.

(4) No que respeita ao **<u>objeto e âmbito de aplicação</u>**:

a) Que a designação conjunta de "*segurança e integridade*" deve ser clarificada, considerando que, de acordo com a definição de segurança da informação, a integridade é uma das suas propriedades fundamentais (**CT 163, ponto 1**);

<u>Entendimento da ANACOM</u>

A referência conjunta a "*segurança e integridade*" respeita o disposto na Lei das Comunicações Eletrónicas, base legal habilitante do presente procedimento regulamentar, sendo, todavia, de admitir que, no âmbito de uma futura revisão deste regulamento e, nomeadamente, após a transposição do Código Europeu das Comunicações Eletrónicas, esta questão seja reequacionada.

b) Que sejam expressamente determinados os serviços de comunicações eletrónicas abrangidos – os "*percecionados como mais importantes para os cidadãos*" – e os serviços excluídos, por irrelevantes (**GRUPO NOS, pág. 18**);

Entendimento da ANACOM

Sobre este ponto e considerando o âmbito de aplicação dos artigos 54.º-A a 54.º-G da Lei das Comunicações Eletrónicas, entende a ANACOM não poder limitar, em geral e *a priori*, o âmbito de aplicação deste projeto.

c) Que não é clarificada a articulação entre a matéria da segurança e integridade e a matéria da emergência, nomeadamente no que respeita ao papel das empresas e das autoridades competentes (**APRITEL, pág. 5**; **GRUPO NOS, págs. 14 e 19**; **RENTELECOM, pág. 3**; **VODAFONE, págs. 7 a 9**);

Entendimento da ANACOM

As matérias relativas à emergência são previstas:

a) Por um lado e enquanto situações extraordinárias, nos casos em que se entende deverem as empresas, no cumprimento do disposto na Lei das Comunicações Eletrónicas e no futuro regulamento, acautelar o cumprimento das suas obrigações nessas matérias, sendo esse o caso, precisamente, do disposto nos n.os 1 e 4 do artigo 2.º do 2.º Projeto;

b) Por outro lado, e atentas as atribuições e competências próprias da ANACOM em matéria de emergência, nos casos em que se entende dever impor medidas específicas às empresas, sendo esse o caso, nomeadamente, do disposto na alínea *e)* do n.º 3 do artigo 8.º e nas alíneas *c)* e *d)* do n.º 1 do artigo 15.º do 2.º Projeto, casos estes em que, ao contrário do que é sustentado, não se entende haver qualquer dúvida quanto ao papel, por um lado, das empresas e, por outro, da ANACOM.

d) Que o projeto se deve limitar aos incidentes que afetam a continuidade dos serviços, não devendo abranger as matérias da confidencialidade das

comunicações e da proteção de dados pessoais (**APRITEL, pág. 5**; **GRUPO NOS, págs. 3 e 18**; **VODAFONE, pág. 8**).

Entendimento da ANACOM

Este projeto – como explicitamente resulta quer da respetiva nota justificativa, quer do respetivo artigo 1.º – tem como base legal habilitante a Lei das Comunicações Eletrónicas, não prejudicando, assim, o disposto no Regulamento Geral sobre a Proteção de Dados ([7]), na Lei n.º 41/2004, de 18 de agosto, na sua redação em vigor, e na demais legislação em vigor aplicável às matérias da privacidade e da proteção de dados pessoais.

Quanto à limitação deste projeto de regulamento aos incidentes de segurança que afetem a continuidade dos serviços, releva-se a definição de segurança das redes e serviços, constante da alínea *m)* do n.º 1 do artigo 3.º do 2.º Projeto, a qual, encontrando-se devidamente alinhada com a prática internacional, inclui outras dimensões para além da continuidade.

(5) Por último e no que respeita às **obrigações de envio de informação** à ANACOM, que as mesmas devem ser eliminadas, atenta a sensibilidade da informação e ao risco de fuga, em particular no que respeita à informação comunicada acerca do inventário de ativos (**APRITEL, pág. 10**; **GRUPO NOS, págs. 13 e 22**; **MEO, pág. 13**; **VODAFONE; pág. 11**).

Entendimento da ANACOM

A ANACOM reconhece a pertinência desta preocupação, pelo que, sem prejuízo do cumprimento das obrigações em causa, é agora prevista a criação de um sistema de informação para o cumprimento das obrigações impostas às empresas,

([7]) Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE.

nomeadamente de notificação, de comunicação, de acesso e de cooperação e partilha de informação, bem como para a gestão da informação por parte da ANACOM, nos termos previstos no n.º 2 do novo artigo 5.º do 2.º Projeto.

3. Propostas apresentadas

No essencial e tendo por base, sobretudo, os comentários gerais submetidos, foram apresentadas, no conjunto das pronúncias, as seguintes **propostas**:

(1) Que deve ser criado um grupo de trabalho para a revisão do projeto (**APRITEL, pág. 9**; **GRUPO NOS, pág. 4**; **VODAFONE, pág. 1**), devendo a mesma ser precedida de uma avaliação de impacto (**APRITEL, pág. 3**; **GRUPO NOS, pág. 12**) e do exercício das competências relevantes da ANACOM, nomeadamente a análise das notificações recebidas, a realização de auditorias de segurança, a obtenção de informações e a realização de investigações (**VODAFONE, pág. 2**);

Entendimento da ANACOM

A ANACOM opta por avançar com a aprovação do 2.º Projeto, dispensando a criação de um grupo de trabalho para este efeito, considerando, por um lado, que já dispõe da informação necessária, identificada acima na parte *2. Comentários gerais*, e, por outro, que a nova abordagem, abaixo exposta e fundamentada, se aproxima, a um nível que se entende adequado, da abordagem detalhadamente proposta pelas empresas nas suas pronúncias.

(2) Que o projeto de regulamento deve antes fixar a prossecução de objetivos de segurança, deixando a definição das medidas concretas ao critério de cada empresa, sugerindo-se, para o efeito, a adoção da metodologia subjacente ao documento *Technical Guideline on Security Measures* (**APRITEL, págs. 6 e 7**; **MEO, págs. 4 e 5**; **GRUPO NOS, págs. 3, 6 e 8 a 10**; **NOWO/ONITELECOM, págs. 2 e 7**; **VODAFONE, pág. 2**) e a adoção de uma aproximação faseada (**MEO, pág. 5**), com

início no nível de sofisticação 1 (*básico*) (**APRITEL, págs. 6 e 7**; **NOWO/ONITELECOM, pág. 2**).

Entendimento da ANACOM

Considerando os comentários gerais apresentados, nomeadamente em matéria de proporcionalidade das medidas impostas no Projeto, entende a ANACOM dever alterar a sua abordagem no âmbito do Título II, nos seguintes termos:

a) A um primeiro nível e como regra geral, determinar que as empresas devem, nomeadamente, adotar todas as medidas de segurança incluídas nos níveis de sofisticação 1 (*básico*) e 2 (*norma de indústria*) para a prossecução de cada um dos 25 objetivos de segurança constantes do novo Anexo ao 2.º Projeto, o qual se baseia, com as necessárias adaptações, no documento *Technical Guideline on Security Measures*, nos termos previstos no n.º 1 do artigo 7.º do 2.º Projeto;

b) A um segundo nível e a título excecional, determinar que, tendo por fundamento os resultados de uma análise dos riscos, uma adequada prossecução de um objetivo de segurança *(i)* não exija, mediante autorização prévia da ANACOM, o cumprimento de uma ou de várias medidas de segurança previstas no nível de sofisticação 2 (*norma de indústria*) ou *(ii)* exija o cumprimento de uma ou de várias medidas de segurança previstas no nível de sofisticação 3 (*estado da técnica*), nos termos previstos, respetivamente, nas alíneas *a)* do n.º 1 e no n.º 2 e na alínea *b)* do n.º 1, ambos do artigo 7.º do 2.º Projeto; e

c) A um terceiro nível, impor um conjunto de 11 medidas específicas que, em qualquer caso e nos termos aplicáveis, devem ser adotadas pelas empresas, elencadas n.º 3 do artigo 7.º e previstas nos artigos 8.º a 19.º do 2.º Projeto.

Através desta abordagem e em termos que se entende poderem ir ao encontro do essencial das preocupações suscitadas nas pronúncias recebidas:

a) Em primeiro lugar, é assim criado um espaço de flexibilidade que deixa ao critério de cada empresa, tendo em consideração os riscos e as ameaças existentes e a sua situação específica, a definição das medidas concretas a

adotar para cumprimento da Lei das Comunicações Eletrónicas e do futuro regulamento, em conformidade com o princípio da adequação que resulta do disposto no artigo 54.º-A daquele diploma;

b) Em segundo lugar e através dessa mesma flexibilidade, permite-se assim, ao adequar o impacto destas medidas à situação específica de cada empresa, garantir um investimento eficiente no cumprimento da Lei das Comunicações Eletrónicas e do futuro regulamento em matéria de segurança e integridade das redes e serviços; e

c) Por último, não deixa de se impor um patamar mínimo de obrigações, quer através da fixação do nível de sofisticação 2 (*norma de indústria*) como regra geral, nos termos previstos no n.º 1 do artigo 7.º do 2.º Projeto, quer através do conjunto de medidas específicas elencadas n.º 3 do artigo 7.º e previstas nos artigos 8.º a 19.º do 2.º Projeto.

De igual modo e através do regime transitório previsto nos n.ºs 2 e 3 do artigo 35.º do 2.º Projeto, permite-se que cada empresa, na medida adequada à sua situação específica, adote uma execução faseada das medidas impostas, contanto que cumpra, no final, os prazos aí fixados.

Nesta solução não se acompanha, porém, a proposta de que, em geral, o patamar mínimo de obrigações corresponda ao nível de sofisticação 1 (*básico*), por se entender que, face à dependência da sociedade e da economia em relação ao funcionamento das redes e serviços de comunicações eletrónicas, se deve assumir como referencial o nível de sofisticação 2 (*norma de indústria*), que corresponde ao padrão seguido pela indústria no âmbito da normalização técnica internacional.

Nem poderia ser de outra forma, sublinhe-se, se atendermos ao facto de que, de acordo com o disposto no n.º 3 do artigo 54.º-C da Lei das Comunicações Eletrónicas e na ausência de decisões da Comissão Europeia (com sublinhado nosso), as medidas impostas "*devem <u>basear-se</u> nas normas europeias e internacionais existentes sobre a matérias*", o que, no entendimento da ANACOM, dificilmente se

coadunaria com a previsão, em geral, de uma base inferior a tal referencial normativo, como seria o caso da previsão, em geral, do nível de sofisticação 1 (*básico*).

Tal não impede, em qualquer caso:

a) Que, na execução das medidas agora preconizadas e dentro dos prazos fixados nos n.os 2 e 3 do artigo 35.º do 2.º Projeto, as empresas adotem um calendário faseado que, pela via que entendam ser mais adequada ao seu caso concreto, evolua do nível de sofisticação 1 (*básico*) para o nível de sofisticação 2 (*norma de indústria*) e, onde necessário ao abrigo do disposto na alínea *b)* do n.º 1 do artigo 7.º do 2.º Projeto, para o nível de sofisticação 3 (*estado da técnica*); e

b) Que, mesmo após o termo desses prazos, tendo por fundamento os resultados de uma análise dos riscos e mediante autorização prévia da ANACOM, as empresas prossigam adequadamente um objetivo de segurança sem o cumprimento de uma ou de várias medidas de segurança previstas no nível de sofisticação 2 (*norma de indústria*), nos termos previstos na alínea *a)* do n.º 1 e no n.º 2, ambos do artigo 7.º do 2.º Projeto.

Ainda sobre esta nova abordagem, salienta-se que a ANACOM, desde o início da formação do Grupo de Peritos do Artigo 13.º-A, tem estado ativamente envolvida nos trabalhos deste grupo, os quais são facilitados pela ENISA e que têm conduzido esta agência europeia à publicação de diversos documentos, designadamente o documento *Technical Guideline on Security Measures*. Foi no âmbito dos seus trabalhos que, até ao momento atual, foram realizadas duas reuniões deste grupo em Portugal, sob os auspícios da ANACOM, respetivamente em fevereiro de 2012 e, mais recentemente, em março de 2016, com o envolvimento e a participação das empresas e associações do setor.

Com esta nova abordagem, a ANACOM reconhece que, dos diversos documentos publicados pela ENISA em resultado dos trabalhos desenvolvidos pelo Grupo de Peritos do Artigo 13.º-A, o documento *Technical Guideline on Security Measures* se destaca como um referencial nesta matéria, sendo ainda de salientar, entre outros e

para efeitos do disposto na alínea *c)* do n.º 2 do artigo 6.º do 2.º Projeto, os relatórios anuais de incidentes (*Annual Incident Reports*) desde 2011, o documento "*Guideline on Threats and Assets"* e o documento "*Technical Guideline on Incident Reporting*".

4. Comentários específicos

4.1. Título I

Quanto às disposições constantes do Título I (*Disposições gerais*), salienta-se, entre outros ([8]), os seguintes **comentários específicos**:

(1) No que respeita ao objeto (**artigo 1.º**), que seja incluída uma referência a um sistema de governo e gestão de risco, por adoção de uma norma internacional (**EDP, pág. 4**);

Entendimento da ANACOM

No que respeita ao objeto, entende a ANACOM dever manter os termos previstos no artigo 1.º, que se encontram devidamente alinhados não só com o disposto na Lei das Comunicações Eletrónicas, que constitui, afinal, a respetiva base legal habilitante, mas também com a estrutura do 2.º Projeto e a delimitação dos respetivos títulos.

(2) No que respeita ao âmbito (**artigo 2.º**):

a) Que a referência aos equipamentos localizados nas instalações dos clientes seja eliminada (**MEO, pág. 9**) ou, pelo menos, restrita aos ativos da propriedade do operador ou que estão sobre a sua gestão e controlo total (**GRUPO NOS,**

([8]) Ver, nomeadamente, CT163, pontos 1 a 4, DELOITTE, ponto II, EDP, pág. 4, EMGFA, ponto 5(a), FCT, GNS/CNCS, pontos 12 e 20 a 22, MEO, págs. 9 e 10, GRUPO NOS, págs. 18 a 20, SRPCBA e VODAFONE, págs. 8 a 10.

pág. 20), ou que sejam identificados os tipos de equipamentos abrangidos (**VODAFONE, pág. 10**);

Entendimento da ANACOM

O disposto no agora n.º 6 do artigo 2.º do 2 .º Projeto, que a ANACOM considera dever manter, encontra-se alinhado com o entendimento subjacente ao disposto na alínea *b)* do n.º 3 do artigo 3.º do Regulamento (UE) 2015/2120 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015, que estabelece medidas respeitantes ao acesso à Internet aberta, nomeadamente quando dispõe (com sublinhados nossos) que cabe aos "*prestadores de serviços de acesso à Internet*" estabelecer medidas de gestão do tráfego "*na medida do necessário, e apenas durante o tempo necessário*" para "*preservar a integridade e a segurança da rede, dos serviços prestados através dela e dos equipamentos terminais dos utilizadores finais*".

Sempre se salienta, em qualquer caso, que a disposição em causa, tanto no Projeto, como no 2.º Projeto, limita os ativos abrangidos aos ativos "*de sua propriedade ou gestão*".

b) Que deve ser garantida a reciprocidade das obrigações para todas as empresas que venham a ser identificadas como operadores de serviços essenciais ou como proprietários ou operadores de infraestruturas críticas, em particular em relação aos fornecedores do setor energético (**VODAFONE, págs. 7 e 8**);

Entendimento da ANACOM

Sem prejuízo da relevância da questão e das diligências que a ANACOM deva realizar para o efeito, no âmbito da prossecução das suas atribuições e competências e, em particular, no âmbito das suas relações de cooperação, designadamente com vista à melhoria da articulação com as empresas do setor energético, relembra-se que, em conformidade com os limites da respetiva base legal habilitante, este projeto de regulamento apenas pode abranger a regulamentação das obrigações das empresas que oferecem redes de

comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público.

c) No que respeita às definições (**artigo 3.º**), que as mesmas devem ser revistas, em particular as definições de «*ativos*», de «*incidente de segurança*», de «*responsável pela segurança*», de «*segurança das redes e serviços*» e de «*vulnerabilidade*», nomeadamente, tendo em conta não só as dúvidas por elas suscitadas, como também a necessidade de assegurar a coerência com termos semelhantes utilizados em documentação diversa, nomeadamente o documento *Technical Guideline on Security Measures* e algumas normas internacionais da série ISO/IEC 27000 (**CT163, pontos 1 a 4**; **EDP, pág. 4**; **EMGFA, ponto 5(a)**; **GRUPO NOS, pág. 20**; **MEO, págs. 9 e 10**; **VODAFONE, pág. 10**);

Entendimento da ANACOM

A ANACOM, tendo em consideração os contributos recebidos, procede à revisão deste artigo, incluindo a adaptação, a introdução e a eliminação de definições, assinalando-se, em particular, o seguinte:

a) Acompanhando a simplificação da disposição relativa à gestão dos riscos, nos termos agora previstos no artigo 10.º do 2.º Projeto, procede-se à eliminação da definição de «*análise dos riscos*»;

b) A definição de «*ativos*», que se mantém, pretende conciliar a noção utilizada no documento *Technical Guideline on Security Measures* com o disposto na Lei das Comunicações Eletrónicas, em particular as definições de rede de comunicações eletrónicas e de serviço de comunicações eletrónicas;

c) A definição de «*incidente de segurança*» pretende conciliar o disposto nas várias disposições da Lei das Comunicações Eletrónicas com a noção utilizada no documento *Technical Guideline on Security Measures,* sendo a mesma, em qualquer caso, objeto de adaptação no 2.º Projeto;

d) Tendo em vista assegurar a coerência com o documento *Technical Guideline on Security Measures*, procede-se à eliminação das definições de «*ameaça*», de «*análise dos riscos*», de «*risco*» e de «*vulnerabilidade*»;

e) Para evitar uma possível confusão entre o disposto no SEGNAC e o disposto neste regulamento, pela utilização simultânea do termo «*responsável pela segurança*», opta-se pela sua alteração para «*responsável da segurança*»;

f) A definição de «*segurança das redes e serviços*» é alinhada com a atual versão do Código Europeu das Comunicações Eletrónicas, abrangendo tanto a segurança de redes, mais ligada a aspetos físicos, como a segurança de informação, mais ligada a aspetos lógicos; e

g) Acompanhando-se a revisão do Título II e a introdução do Anexo, acrescenta-se novas definições para *«clientes relevantes»*, «*colaboradores*», «*colaboradores-chave*», «*nível de sofisticação 1*», «*nível de sofisticação 2*» e «*nível de sofisticação 3*».

Por último e atendendo às dúvidas suscitadas, o anterior n.º 2 do artigo 3.º do Projeto é eliminado.

d) No que respeita à cooperação e partilha de informação (**artigo 4.º**), que é necessário clarificar o papel da ANACOM em matéria de resposta a incidentes e assegurar a articulação com o CERT.PT (**GNS/CNCS, pontos 21 e 22**) e com outros setores (**EDP, pág. 4**), bem como clarificar o que se entende quanto ao efeito em cascata (**DELOITTE, ponto II**).

Entendimento da ANACOM

Quanto à articulação com o CERT.PT e à clarificação do papel da ANACOM em matéria de resposta a incidentes, remete-se, respetivamente, para o disposto no novo artigo 20.º e no novo n.º 3 do artigo 16.º, ambos do 2.º Projeto.

Quanto à cooperação com outros setores e como acima ficou referido, relembra-se que, em conformidade com os limites da respetiva base legal habilitante, este projeto

de regulamento apenas pode abranger a regulamentação das obrigações das empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público.

Por último e no que respeita ao efeito em cascata e com vista a evitar dúvidas na sua interpretação, clarifica-se a redação da alínea *b)* do n.º 2 do artigo 4.º, ao mesmo tempo que – tendo em consideração a experiência recolhida pela ANACOM nos últimos anos – se reforça, em especial, o dever de cooperação entre empresas no caso da ocorrência de um ou mais incidentes de segurança, através da nova alínea *a)* do mesmo n.º 2 e em articulação com o disposto no n.º 15 do artigo 22.º

4.2. Título II

Quanto às disposições constantes do Título II (*Obrigações das empresas em matéria de segurança e integridade*) e remetendo-se, antes de mais, para o acima exposto em *3. Propostas de abordagem*, salienta-se:

a) Que as disposições gerais, constantes do Capítulo I deste título, são objeto de revisão com vista a refletir a nova abordagem adotada nesta matéria, nos termos previstos nos artigos 6.º e 7.º do 2.º Projeto;

b) Que, em articulação com o disposto no n.º 1 do artigo 7.º, é introduzido um Anexo ao 2.º Projeto, do qual constam agora os objetivos de segurança a prosseguir e, para a prossecução de cada um deles, as medidas de segurança a adotar, tendo por base, com as devidas adaptações, o documento *Technical Guideline on Security Measures*;

c) Que, no que respeita às medidas específicas constantes do Capítulo II deste título:

- São eliminados 6 artigos, designadamente os anteriores artigos 10.º (*Medidas de redundância, de robustez e de resiliência*), 12.º (*Procedimentos de gestão de alterações*), 13.º (*Sistemas de controlos de acesso*), 14.º (*Sistema de monitorização e controlo*), 17.º (*Caracterização geral de segurança*) e 23.º (*Dossier de segurança*), em todos os casos sem prejuízo da disciplina das

matérias em causa, nos termos agora previstos nos artigos 6.º e 7.º e no Anexo do 2.º Projeto; e

- São revistos e reorganizados os restantes 12 artigos, de acordo com o elenco agora constante do n.º 3 do artigo 7.º do 2.º Projeto.

Neste contexto e passando à análise das pronúncias recebidas quanto ao Título II, salienta-se, entre outros ([9]), os seguintes **comentários específicos**:

(1) No que respeita às disposições gerais (**artigos 6.º e 7.º**), que as obrigações das empresas se devem basear em normas técnicas reconhecidas internacionalmente, que os referenciais normativos a estabelecer no Título II e no Título IV devem ser articulados e que a metodologia para a sua determinação e publicação deve ser revista (**CT163, pontos 11 e 14**; **EDP, pág. 4**; **GRUPO NOS, págs. 20 e 21**);

Entendimento da ANACOM

Considerando os contributos recebidos, a ANACOM opta por incluir, no 2.º projeto, uma lista não exaustiva das normas a considerar para efeitos do disposto quer das obrigações das empresas, nos termos previstos na alínea *b)* do n.º 2 do artigo 6.º, quer dos documentos e normas de referência no âmbito das auditorias de segurança, nos termos previstos no artigo 27.º

As listas incluídas baseia-se em normas, especificações e recomendações nacionais, europeias e internacionais existentes sobre a matéria.

Para além disso, a ANACOM destaca, ainda, que o documento *Technical Guideline on Security Measures* – no qual é baseada, com as devidas adaptações, a

([9]) Ver, nomeadamente, APRITEL, págs. 10 a 12, CT163, pontos 5 a 9, 11 e 14, DECO, ponto II.1, DELOITTE, ponto II, EDP, págs. 4 a 6, EMGFA, ponto 5(b), FCT, pontos a) e f), GNS/CNCS, ponto 18, MEO, págs. 11 a 17, GRUPO NOS, págs. 20 a 28, NOWO/ONITELECOM, pág. 3, RENTELECOM, págs. 2 e 3, SGMAI, SRPCBA e VODAFONE, págs. 10 a 13.

abordagem prevista no n.º 1 do artigo 7.º e no novo Anexo do projeto – se suporta também, por seu turno, em normativo técnico internacional, designadamente as normas da série ISO/IEC 27000, a norma ISO 22310 e recomendações da União Internacional das Telecomunicações, tendo também em conta algumas normas nacionais e outras boas práticas.

(2) No que respeita à classificação de ativos (**artigo 8.º**) e ao inventário de ativos (**artigo 9.º**), que os mesmos são excessivamente complexos e onerosos e de difícil articulação com outras medidas previstas no projeto, designadamente as medidas relativas à gestão dos riscos (**APRITEL, pág. 10**; **CT 163, pontos 6 e 7; DELOITTE, ponto II**; **MEO, págs. 11 a 13**; **GRUPO NOS, págs. 21 e 22**; **NOWO/ONITELECOM, pág. 3**; **VODAFONE, págs. 10 e 11**);

Entendimento da ANACOM

Antes de mais, a ANACOM considera, à semelhança dos pressupostos assumidos na documentação técnica publicada pela ENISA, que um dos aspetos basilares em termos da implementação das medidas de segurança das redes e serviços de comunicações eletrónicas é uma caracterização clara dos ativos que são abrangidos e da sua inventariação.

Nesta medida e concordando com a relevância do conteúdo dos comentários recebidos, procede-se à simplificação e à clarificação do procedimento de classificação de ativos, nos seguintes termos:

a) Eliminação da anterior classe C;

b) Agregação, na classe A, das anteriores classes A e B, nos termos previstos nos n.os 2 e 3 do artigo 8.º do 2.º Projeto;

c) Criação de uma nova classe B, nos termos previstos no n.º 4 do artigo 8.º do 2.º Projeto; e

d) Transformação da anterior classe D na nova classe C, nos termos previstos no n.º 5 do artigo 8.º do 2.º Projeto.

Na prática e no sentido da proposta de uma classificação binária, tendo por base um critério de criticidade dos ativos, apresentada em várias pronúncias, deste novo sistema resulta a distinção entre:

a) Por um lado, os ativos críticos, que passam a corresponder ao conjunto dos ativos classificados nas classes A e B – os ativos da classe A por disposição do regulamento e os ativos da classe B em resultado da análise feita por cada empresa relativamente aos seus ativos; e

b) Por outro lado, os restantes ativos, que passam a corresponder aos ativos classificados na classe C.

De forma similar e com um intuito de simplificação, clarifica-se que, ao nível do inventário de ativos, devem do mesmo constar todos os ativos abrangidos, de acordo com a definição constante da alínea *a)* do artigo 3.º do 2.º Projeto, diferenciando-se, porém, a informação que deve constar do inventário de ativos relativamente, por um lado, aos ativos das classes A, B e C – mais simples, nos termos previstos no n.º 2 do artigo 9.º do 2.º Projeto – e, por outro lado, aos ativos das classes A e B – mais complexa, nos termos previstos no n.º 3 do mesmo artigo.

(3) No que respeita à gestão dos riscos (**artigo 10.º**), que a obrigação de "*análise dos riscos*" deve ser revista, nomeadamente quanto à delimitação do seu âmbito e periodicidade, tendo em conta a exigência e a complexidade do projeto, à identificação da metodologia nacional relevante e à clarificação da distinção entre análises de risco globais e parciais e do papel da ANACOM no âmbito destas últimas (**APRITEL, págs. 10 e 11**; **CT163, ponto 8**; **DELOITTE, ponto II**; **EDP, pág. 5**; **FCT, ponto a)**; **MEO, págs. 13 e 14**; **GRUPO NOS, págs. 22 a 24**; **NOWO/ONITELECOM, pág. 3**; **RENTELECOM, págs. 2 e 3**; **VODAFONE, págs. 11 e 12**);

Entendimento da ANACOM

Em coerência com a nova abordagem projetada, nos termos acima expostos e fundamentados na parte *3. Propostas apresentadas*, e sempre se destacando a importância da gestão dos riscos para efeitos da eficiência e eficácia das medidas de segurança adotadas pelas empresas, a ANACOM procede à redução desta

disposição a uma obrigação de revisão da metodologia de gestão dos riscos, nos termos agora previstos no artigo 10.º do 2.º Projeto, sem prejuízo das obrigações que, nesta matéria, agora resultam dos artigos 6.º e 7.º e, em especial, do Anexo.

(4) No que respeita aos procedimentos de controlo da gestão excecional de tráfego de acesso à Internet (**artigo 11.º**), que os mesmos assumem um caráter excessivo e de difícil exequibilidade técnica, com preocupações em termos de interceção de tráfego, e que é necessário clarificar o disposto neste artigo no respeitante à priorização de tráfego e à reserva de capacidade (**FCT, ponto f)**; **MEO, pág. 15**; **GRUPO NOS, pág. 25**; **VODAFONE, pág. 12**);

Entendimento da ANACOM

A introdução deste artigo no projeto de regulamento resulta, fundamentalmente, do disposto no Regulamento (UE) 2015/2120 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015, que estabelece medidas respeitantes ao acesso à Internet aberta, bem como das linhas orientadoras elaboradas pelo *Body of European Regulators for Electronic Communications* (*BEREC*) no respeitante às situações de exceção previstas no n.º 3 do respetivo artigo 3.º, considerando a necessidade de dar forma à sua implementação, na estrita medida em que o mesmo releva no âmbito da matéria relativa à segurança e integridade das redes e serviços de comunicações eletrónicas.

Considerando as dúvidas suscitadas, a ANACOM procede, em qualquer caso, à eliminação do anterior n.º 4.

(5) No que respeita aos exercícios (**artigo 12.º**), que a periodicidade anual é excessiva e disruptiva para a atividade das empresas e que deve caber às mesmas proceder ao desenho do modelo de testes a desenvolver, incluindo o seu faseamento em termos de ativos abrangidos, tendo em conta eventuais riscos inerentes à sua realização, devendo caber à ANACOM apenas a dinamização e a coordenação de exercícios conjuntos (**APRITEL, págs. 11 e 12**; **MEO, pág. 16**; **GRUPO NOS, págs. 25 e 26**; **NOWO/ONITELECOM, pág. 3**; **VODAFONE, pág. 13**);

Entendimento da ANACOM

Sem prejuízo de considerar que a realização de exercícios é fundamental para o treino das equipas e para a eficácia das medidas de segurança adotadas pelas empresas, a ANACOM procede à simplificação das obrigações nesta matéria, nomeadamente alterando-se para uma periodicidade máxima bianual e distinguindo-se, num novo número, a matéria da participação em exercícios conjuntos, nos termos agora previstos no artigo 12.º do 2.º Projeto.

(6) No que respeita à informação aos clientes relevantes (**artigo 13.º**), que não se identifica qualquer vantagem, nem tão pouco fundamento, para a sua imposição (**GRUPO NOS, pág. 26**) e que a sua comunicação à ANACOM não só é redundante em face do disposto em matéria de notificações de violações de segurança ou perdas de integridade com impacto significativo (**GRUPO NOS, pág. 26**), como coloca em causa obrigações contratuais de confidencialidade (**MEO, pág. 16**);

Entendimento da ANACOM

Em matéria de informação aos clientes relevantes, é entendimento da ANACOM que, face, por um lado, à criticidade dos serviços prestados pelos clientes em causa e, por outro, ao aumento da dependência da prestação desses serviços em relação às redes e serviços de comunicações eletrónicas em que se suportam, é fundamental manter – e até reforçar – as disposições relativas à sua proteção no 2.º Projeto. Tal não prejudica, porém, que se proceda a uma simplificação do disposto neste artigo, nomeadamente limitando o âmbito dos incidentes em causa e excluindo as situações de reação a ameaças ou a vulnerabilidades.

Quanto às obrigações contratuais de confidencialidade e como tem sido a posição firme desta Autoridade, as mesmas, por si só, não obstam à comunicação de informação à ANACOM ao abrigo do disposto em normas legais ou regulamentares aplicáveis e na medida necessária à prossecução das suas atribuições e ao exercício das suas competências.

(7) No que respeita ao responsável da segurança (**artigo 14.º**), que o seu regime deve ser revisto, nomeadamente no que respeita à sua localização, à sua interação com a

ANACOM, à possibilidade de designação de um adjunto e às suas qualificações (**CT163, ponto 9**; **DELOITTE, ponto II**; **GRUPO NOS, pág. 27**);

Entendimento da ANACOM

Tendo em conta os contributos recebidos, a ANACOM procede à revisão da função de responsável de segurança, quer no artigo 14.º do 2.º Projeto, onde se salienta, em particular, a introdução da função de adjunto, quer no artigo 18.º do 2.º Projeto, no que respeita aos deveres específicos de comunicação à ANACOM.

(8) No que respeita ao ponto de contacto permanente (**artigo 15.º**), que deve ser agilizado, através deste ponto de contacto, o acesso dos operadores de serviços essenciais às empresas que oferecem redes e serviços de comunicações eletrónicas (**EDP, págs. 5 e 6**) e que o respetivo regime deve ser simplificado no que respeita ao ponto de contacto alternativo (**MEO, pág. 17**; **GRUPO NOS, pág. 27**);

Entendimento da ANACOM

Tendo em consideração os contributos recebidos, procede-se à revisão do disposto nesta matéria, nos artigos 15.º e 18.º do 2.º Projeto, nomeadamente diferenciando o regime para as empresas que detenham ativos classificados nas classes A – neste caso, em regime de disponibilidade contínua – e para as restantes empresas – neste caso, em regime de disponibilidade contínua limitada a períodos de ativação –, desenvolvendo as suas funções e eliminando a função de ponto de contacto alternativo.

No que respeita à questão do acesso aos pontos de contacto permanente por parte dos operadores de serviços essenciais, remete-se para o "*Relatório do Grupo de Trabalho dos Incêndios Florestais – Medidas de Proteção e Resiliência de Infraestruturas de Comunicações Eletrónicas*", nomeadamente no respeitante a procedimentos intersetoriais para deteção, resposta e mitigação.

(9) No que respeita à equipa de resposta a incidentes de segurança (**artigo 16.º**), que é necessário clarificar o seu regime, nomeadamente em relação à questão do acesso

e à limitação da sua intervenção à resposta a incidentes de segurança que impliquem interrupção dos serviços (**MEO, pág. 17**; **GRUPO NOS, pág. 28**);

Entendimento da ANACOM

Tendo em consideração os comentários recebidos, a ANACOM procede à revisão desta disposição, nos termos agora previstos no artigo 16.º do 2.º Projeto, nomeadamente determinando que as empresas que detenham ativos classificados nas classes A devem dispor de uma equipa de resposta a incidentes de segurança que afetem os respetivos ativos classificados nas classes A ou B.

No que respeita à limitação do âmbito de intervenção à resposta a incidentes de segurança que impliquem interrupção dos serviços, remete-se para o acima exposto na alínea *d)* do ponto *(4)* da parte *1. Comentários gerais*.

(10) No que respeita ao plano de segurança (**artigo 17.º**), que o mesmo deve ser definido pelas empresas de acordo com o âmbito das suas redes e serviços e os objetivos de segurança e níveis de resiliência estabelecidos internamente e que a sua revisão anual é excessiva, sugerindo-se que passe a bianual (**MEO, pág. 16**).

Entendimento da ANACOM

Tendo em consideração os comentários recebidos e sem prejuízo de considerar que o plano de segurança é fundamental para as empresas, a ANACOM procede à revisão desta disposição, nos termos agora previstos no artigo 17.º do 2.º Projeto, bem como à eliminação do prazo mínimo de revisão do relatório, sem prejuízo da obrigação de o manter atualizado.

4.3. Título III

Quanto às disposições constantes do Título III (*Obrigações de notificação e de informação ao público*), salientamos, entre outros ([10]), os seguintes **comentários específicos**:

(1) No que respeita às circunstâncias das obrigações de notificação (**artigo 21.º**):

a) Que existe a necessidade de algumas entidades serem também destinatárias da informação relativa a violações de segurança ou perdas de integridade com impacto significativo, na medida necessária à prossecução das suas atribuições (**PGR**) ou à prestação dos seus serviços (**EDP, págs. 2, 5 e 6**);

b) Que as circunstâncias originadoras da obrigação de notificação à ANACOM devem ser revistas, nomeadamente no sentido do seu alargamento (**EDP, págs. 2, 5 e 6; EMGFA, ponto 5(c)**; **SGMAI**) ou no sentido da sua adaptação ou eliminação, designadamente as circunstâncias relativas aos patamares inferiores (**GRUPO NOS, pág. 30**), as circunstâncias que resultem de uma atividade programada (**MEO, pág. 17**) e as circunstâncias relativas a clientes relevantes (**MEO, pág. 18**; **GRUPO NOS, págs. 28 e 29**);

c) Que os patamares relativos às circunstâncias originadoras da obrigação de notificação à ANACOM sejam revistos, fixando-os em termos relativos e não absolutos (**CT 163, ponto 6**);

d) Que existe a necessidade de alinhamento com o regime a ser previsto na legislação nacional de transposição 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 (**FCT, ponto b)**; **GNS/CNCS, pontos 13 a 17**);

([10]) Ver, nomeadamente, DECO, ponto II.2, EDP, págs. 2, 5 e 6, EMGFA, ponto 5(c), FCT, pontos b), c) e d), GNS/CNCS, pontos 13 a 17, GRUPO NOS, págs. 28 a 30, MEO, págs. 17 a 19, PGR e SGMAI.

Entendimento da ANACOM

Tendo em conta o sentido diverso dos contributos recebidos, bem como, sobretudo, a experiência recolhida até ao momento, a ANACOM considera ser de manter as circunstâncias originadoras da obrigação de notificação de violações de segurança ou perdas de integridade com impacto significativo, bem como os respetivos patamares, nos termos agora previstos no artigo 21.º do 2.º Projeto.

A tendência cada vez mais marcante do aumento da dependência da sociedade, em geral, e, em especial, de determinadas entidades que prestam serviços relevantes e cujos processos críticos dependem das condições de funcionamento das redes e serviços de comunicações eletrónicas, tem vindo a corroborar a adequação deste mecanismo de notificação, com o objetivo de manter a ANACOM informada da situação do setor e do seu impacto socioeconómico e de assim permitir uma cabal prossecução das suas atribuições.

No que respeita ao alargamento dos sujeitos destinatários, remete-se para o disposto no artigo 20.º e no objetivo n.º 18 do Anexo do 2.º Projeto, bem como, no que respeita, em particular, ao Ministério Público, a introdução da nova alínea *l)* do n.º 9 do artigo 22.º do 2.º Projeto.

No que respeita ao alargamento do elenco de clientes agora constante do n.º 5 do artigo 21.º do 2.º Projeto, salienta-se que, de acordo com o disposto nesse número, a ANACOM pode proceder à identificação de outras entidades, com base numa análise a realizar caso a caso.

Por último e no que respeita ao alinhamento com o regime a ser previsto na legislação nacional de transposição 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, ainda em discussão, a ANACOM concorda com a necessidade de articular os regimes de âmbito setorial entre si, bem como de promover a coerência entre os mesmos e, em geral e entre outros, com os regimes de planeamento de emergência de proteção civil, de planeamento civil de emergência e de cibersegurança.

Em particular e nos termos agora constantes do novo n.º 4 do artigo 19.º do 2.º Projeto, a definição da taxonomia comum aí prevista, bem como do formato em que a informação deve ser apresentada, por parte da ANACOM, terá necessariamente em consideração a articulação com o modelo assumido em matéria de cibersegurança.

Realça-se, em qualquer caso, que o presente projeto de regulamento não impõe – nem poderia impor – obrigações de notificação aos operadores de serviços essenciais, antes alargando a obrigação imposta às empresas que oferecem redes e serviços de comunicações eletrónicas a circunstâncias específicas relativas ao impacto nos serviços por si prestados àqueles operadores, nos termos previstos na alínea *f)* do n.º 2 e no n.º 5 do artigo 21.º do 2.º Projeto.

(2) No que respeita ao formato e aos procedimentos aplicáveis em matéria de notificação de violações de segurança ou de perdas de integridade (**artigo 22.º**):

a) Que se preveja a possibilidade de envio à ANACOM da notificação final por meios eletrónicos, permitindo-se a utilização de uma assinatura digital pelo responsável da segurança (**GRUPO NOS, pág. 30**);

b) Que se inclua causas raiz adicionais (**MEO, pág. 18**);

c) Que se informe atempadamente as empresas de eventuais alterações dos contactos da ANACOM para efeitos de envio de notificações (**MEO, pág. 18**);

d) Que se elimine a obrigatoriedade de contacto telefónico e se envie às empresas uma confirmação de receção de uma notificação (**MEO, pág. 18**);

Entendimento da ANACOM

Concordando-se com a pertinência das sugestões em causa, procede-se:

- À previsão da possibilidade de envio de notificação final por meios eletrónicos, em termos a determinar pela ANACOM, que possibilita a utilização de assinatura digital pelo Responsável da Segurança, nos termos legalmente previstos, em conformidade com o agora disposto no n.º 13 do artigo 22.º do 2.º Projeto; e

- À introdução de um novo n.º 14 no artigo 22.º do 2.º Projeto, com o regime de alteração de contactos por parte da ANACOM.

Não se acompanha, porém, as propostas relativas:

- À introdução de novas causas raiz adicionais, por se entender dever manter o alinhamento, nesta matéria, com a documentação da ENISA e não se constatar necessidade de adaptação resultante de alguma característica especial do país;

- À eliminação da obrigatoriedade de contacto telefónico, pela segurança que o mesmo tem oferecido em termos de redundância; e

- À introdução de uma confirmação de receção de uma notificação, que se entende dever ser de considerar no âmbito do desenvolvimento do sistema de informação previsto nos termos do n.º 2 do artigo 5.º do 2.º Projeto.

Por último e tendo por base a experiência da ANACOM no tratamento das notificações, aproveita-se a oportunidade, para introduzir, entre outras alterações ao referido artigo 22.º do 2.º Projeto, as seguintes:

- Priorização do restabelecimento das comunicações aos clientes relevantes, nos termos previstos na parte final do n.º 4 e na alínea *b)* do objetivo n.º 19 do Anexo, sujeitos ao disposto no n.º 7 do artigo 35.º;

- Introdução da subalínea *iv)* da alínea *f)* do n.º 5, das alíneas *c)* e *d)* no n.º 7, das subalíneas *iv)* e *vii)* da alínea *e)*, da alínea *k)* e da alínea *l)* do n.º 9, no âmbito do conteúdo das notificações, com vista à melhoria da informação recolhida por via das notificações dirigidas à ANACOM, nomeadamente nas matérias de impacto geográfico, de afetação de clientes relevantes e de denúncia criminal;

- Adaptação do disposto na subalínea *i)* da alínea *e)* do n.º 9 às alterações introduzidas em matéria de classificação de ativos; e

- Introdução do dever de comunicação à ANACOM da resolução total da situação residual, quando exista, nos termos previstos no novo n.º 10.

(3) No que respeita às condições aplicáveis em matéria das obrigações de informação ao público (**artigo 23.º**), que existe a necessidade de enquadrar incidentes de afetação individual de clientes, nomeadamente operadores de serviços essenciais, com ou sem impacto disruptivo (**EDP, pág. 6**);

Entendimento da ANACOM

Sobre este ponto, remete-se para o disposto, por um lado, na alínea *f)* do n.º 2 e no n.º 5 do artigo 21.º do 2.º Projeto, onde se preveem circunstâncias de afetação individual de clientes, bem como, por outro lado, no respetivo artigo 13.º, onde se prevê um dever específico de comunicação a esses mesmos clientes, os quais incluem, precisamente, os operadores de serviços essenciais.

No mesmo sentido, mais se salienta que é fixada a priorização do restabelecimento dos serviços a esses clientes, no n.º 4 do artigo 22.º do 2.º Projeto, assim como são revistos os conteúdos das notificações dirigidas à ANACOM com vista a evidenciar o impacto nos mesmos, nomeadamente na subalínea *iv)* da alínea *f)* do n.º 5, na subalínea *iii)* da alínea *d)*, na subalínea *iv)* da alínea *e)* e na subalínea iii) da alínea *k)* do n.º 9, todos do referido artigo.

(4) No que respeita ao conteúdo, aos meios e aos prazos de divulgação (**artigo 23.º**), que seja incluída informação sobre políticas de gestão de tráfego e situações de congestionamento de rede (**DECO, ponto II.1**) e que seja revista a exigência do horário alargado das 09:00 às 19:00 (**MEO, págs. 18 e 19**).

Entendimento da ANACOM

Tendo em consideração a experiência recolhida com os incêndios ocorridos em 2017 e os contributos recebidos, a ANACOM entende dever alterar a redação do projeto de regulamento nesta matéria, agora constante do artigo 24.º do 2.º Projeto, com o objetivo de melhorar a informação sobre o estado de funcionamento das redes e dos serviços na sequência de violações de segurança ou perdas de integridade com impacto significativo, disponibilizada pelas empresas ao público.

Neste contexto e atendendo ao caráter contínuo da utilização de redes e serviços de comunicações eletrónicas, entende-se não ser de aceitar a proposta de redução do horário previsto na alínea *c)* do n.º 1 do artigo 24.º do 2.º Projeto, tendo-se, antes, procedido à sua substituição por um regime contínuo e pela redução do prazo de divulgação de 4 horas úteis para 1 hora após a notificação inicial à ANACOM.

Não se acompanha, de igual modo, a proposta de divulgação ao público das políticas de gestão de tráfego e das situações de congestionamento de rede, por se tratar de matéria prevista no Regulamento (UE) 2015/2120 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015, que estabelece medidas respeitantes ao acesso à Internet aberta.

4.4. Título IV

Quanto às disposições constantes do Título IV (*Auditorias à segurança das redes e serviços*), salientamos, entre outros ([11]), os seguintes **comentários específicos**:

(1) A **título geral**, que as auditorias devem poder ter uma configuração de *self-assessment* ou de auditoria interna, com vista a uma minimização de custos e a um aproveitamento do conhecimento interno dos sistemas, dos processos e dos procedimentos já implementados pelas empresas (**APRITEL, pág. 12**; **GRUPO NOS, pág. 31**; **NOWO/ONITELECOM, págs. 3 e 4**);

Entendimento da ANACOM

Apesar de esta Autoridade reconhecer que a utilização de auditores internos permitiria ir ao encontro das preocupações manifestadas pelas empresas relativas à

([11]) Ver, nomeadamente, APRITEL, págs. 12 e 13, CT80, CT163, pontos 10 a 12 e 14, DELOITTE, ponto II, EDP, pág. 8, GNC/CNCS, ponto 20, GRUPO NOS, págs. 20 e 21 e 30 e 31, MEO, pág. 19, NOWO/ONITELECOM, págs. 3 e 4 e VODAFONE, pág. 14.

necessidade de redução do impacto financeiro destas medidas, relembra-se que o Título IV, ao ter por base legal habilitante o disposto nos n.os 1 e 2 do artigo 54.º-F da Lei das Comunicações Eletrónicas, pretende regulamentar a realização de auditorias "*através de entidades auditoras independentes*".

(2) A **título geral**, que os prazos estabelecidos são demasiado otimistas, não levando em consideração a necessidade de as empresas estabelecerem os âmbitos e contratualizarem as auditorias com terceiros (**DELOITTE, ponto II**);

Entendimento da ANACOM

Este comentário é considerado na revisão do Título IV, sem prejuízo da manutenção do prazo global de 2 anos para o ciclo de auditoria, nos termos previstos na alínea *b)* n.º 2 do artigo 31.º do 2.º Projeto, de acordo com a posição da ENISA de que "*preventive audits are usually done at fixed intervals, periodically"* e que, "*in the case of certification (see above) audits are carried out yearly or bi-yearly*" ([12]), procedendo-se à revisão dos restantes prazos individuais no sentido do seu alargamento, nomeadamente nos termos agora previstos nas alíneas *a)* e *b)* do n.º 2 do artigo 31.º, nos n.os 1 e 4 do artigo 32.º e no n.º 1 do artigo 33.º, todos do 2.º Projeto.

(3) A **título geral**, que as auditorias devem ser inseridas num ciclo de melhoria contínua, considerando os planos de evolução tecnológica implementados pelas empresas, e que o plano de correção das não conformidades deve ter em conta a razoabilidade dos investimentos e contemplar os prazos necessários para a sua resolução (**APRITEL, pág. 12**; **GRUPO NOS, pág. 31**; **NOWO/ONITELECOM, pág. 3**);

Entendimento da ANACOM

Este comentário, no que respeita ao ciclo de melhoria contínua, é expressamente acolhido no artigo 26.º do 2.º Projeto, considerando esta Autoridade que a sua

([12]) Pág. 32 do documento *Technical Guideline on Security Measures*.

adoção é útil para a segurança das redes e dos serviços, devendo refletir-se não só ao nível das auditorias, mas também, em termos globais, da estratégia de segurança a seguir pelas empresas.

No que respeita ao disposto no n.º 3 do artigo 33.º do 2.º Projeto, salienta-se que o prazo máximo aí previsto é determinado pela ANACOM e apenas caso assim o entenda, e, como tal, obedece necessariamente a um juízo de adequação, nomeadamente em relação às medidas que concretamente constem do plano de correção das não conformidades.

(4) No que respeita ao âmbito subjetivo e objetivo de aplicação do dever de realização de auditorias (**artigos 25.º e 26.º**), que a definição dos ativos é determinante da complexidade das auditorias (**VODAFONE, pág. 14**) e que estas se devem basear numa amostra (**NOWI/ONITELECOM, pág. 3**);

Entendimento da ANACOM

Concordando com a relevância da definição dos ativos para a complexidade das auditorias, mas optando por mantê-la, considerada a sua aproximação à abordagem adotada no documento *Technical Guideline on Security Measures*, entende, ainda assim, a ANACOM, em linha com as alterações ao artigo 8.º do 2.º Projeto em matéria de classificação de ativos:

a) Por um lado, limitar o âmbito subjetivo de aplicação do dever de realização de auditorias às empresas que detenham ativos classificados na classe A, nos termos agora previstos no artigo 25.º do 2.º Projeto; e

b) Por outro lado, limitar o âmbito objetivo de aplicação do dever de realização de auditorias a uma amostra adequada dos ativos classificados nas classes A e B, nos termos agora previstos no artigo 26.º do 2.º Projeto.

Tal limitação do âmbito de aplicação justifica-se por se tratar dos ativos que, em caso de perturbação no seu funcionamento e atenta a sua criticidade, maior impacto terão para os interesses dos cidadãos.

(5) No que respeita à identificação dos documentos e normas de referência (**artigo 27.º**), que devem ser adotadas normas ISO, nomeadamente normas da série ISO/IEC 27000 (**CT163, ponto 10**; **DELOITTE, ponto II, EDP, pág. 8, NOWO/ONITELECOM, pág. 3**) e normas do âmbito da qualidade (**CT80**), bem como que o respetivo

processo de identificação e de publicação deve ser revisto (**CT163, ponto 11**; **DELOITTE, ponto II; GNS/CNCS, ponto 20; GRUPO NOS, págs. 20 e 21**);

Entendimento da ANACOM

Considerando os contributos recebidos, a ANACOM opta por incluir, no 2.º Projeto, uma lista não exaustiva dos documentos e normas a considerar para efeitos do disposto quer nas obrigações das empresas, nos termos previstos na alínea *b)* do n.º 2 do artigo 6.º, quer nos documentos e normas de referência no âmbito das auditorias de segurança, nos termos previstos no artigo 27.º

(6) No que respeita às auditoras (**artigo 28.º**), que cada auditora seja contratada, no máximo, por apenas 3 anos consecutivos (**CT163, ponto 10**) e que se assegure a inexistência de conflitos de independência, nos termos da lei (**DELOITTE, ponto II**);

Entendimento da ANACOM

Concordando-se com as propostas apresentadas, a redação do n.º 2 do artigo 28.º do 2.º Projeto é revista, no que respeita a conflitos de interesse, sendo aditado um novo n.º 3 ao mesmo artigo com vista a assegurar a rotatividade na escolha das auditoras, determinando-se, atento o prazo global de 2 anos para o ciclo de auditoria, que a mesma auditora não pode realizar mais do que duas auditorias consecutivas.

(7) No que respeita ao dever de colaboração (**artigo 29.º**), que o acesso, por parte da ANACOM, aos fornecedores seja feito por intermédio das empresas (**APRITEL, pág. 13**; **GRUPO NOS, pág. 31**) e apenas em caso de sérias e fundamentadas dúvidas (**GRUPO NOS, pág. 31**);

Entendimento da ANACOM

Sem prejuízo das alterações introduzidas ao artigo 29.º do 2.º Projeto, em particular na alínea *g)* do n.º 1, no n.º 2 e no novo n.º 3, salienta-se que, nos termos da lei, o acesso às auditoras, aos fornecedores e aos colaboradores, assim como a realização de reuniões e a prestação de esclarecimentos, nos termos previstos no referido n.º

2, apenas será solicitado pela ANACOM se necessário para o exercício das suas competências.

(8) No que respeita ao acompanhamento das auditorias pela ANACOM (**artigo 32.º, n.º 2**), que os seus colaboradores devem estar sujeitos ao regime aplicável às auditoras, nomeadamente em relação à sua credenciação e à entrega de declarações de inexistência de conflitos de interesse (**MEO, pág. 19**);

Entendimento da ANACOM

Este comentário é acolhido no que respeita à credenciação dos colaboradores da ANACOM, nos termos agora previstos no n.º 2 do artigo 32.º do 2.º Projeto, remetendo-se, no entanto e quanto a conflitos de interesse, para o regime constante do Capítulo V dos Estatutos, em particular para o respetivo artigo 43.º em matéria de incompatibilidades e impedimentos.

(9) No que respeita ao relatório da auditoria (**artigo 32.º, n.ºs 3 e seguintes**), que o prazo de 10 dias úteis para o respetivo envio deve ser contado a partir da aceitação do relatório pela empresa e não a partir da conclusão das atividades da fase de auditoria (**GRUPO NOS, pág. 30**).

Entendimento da ANACOM

Atendendo ao contributo recebido, a ANACOM opta por, mantendo a data a partir da qual se conta o prazo de envio do relatório de auditoria, alargá-lo de 10 para 20 dias úteis, nos termos agora previstos no n.º 4 do artigo 32.º, realçando-se ainda, a este propósito, a simplificação do conteúdo deste relatório, nos termos agora previstos no n.º 3 do mesmo artigo.

4.5. Título V

Quanto às disposições constantes do Título V (*Disposições finais e transitórias*), foram apresentados os seguintes **comentários específicos**:

(1) No que respeita ao regime sancionatório (**artigo 34.º**), que as contraordenações previstas na Lei das Comunicações Eletrónicas não se encontram devidamente mapeadas com os requisitos previstos no projeto de regulamento (**CT163, ponto 13**);

Entendimento da ANACOM

As contraordenações encontram-se legalmente previstas nas alíneas *u)*, *v)*, *x)* ou *z)* do n.º 3 do artigo 113.º da Lei das Comunicações e o seu mapeamento com as obrigações previstas no Projeto decorre da norma legal habilitante das disposições que as preveem, conforme é explicitado na nota justificativa, no artigo 1.º e ao longo do regulamento, em especial nos artigos 6.º, 7.º, 20.º e 23.º do 2.º Projeto.

(2) No que respeita ao regime transitório (**artigo 35.º**), que alguns dos prazos aí previstos não são adequados ao tempo necessário à adaptação das empresas, em particular no que respeita à classificação dos ativos e à elaboração do inventário de ativos (**MEO, págs. 19 e 20; VODAFONE, pág. 14**), bem como ao sistema de controlo de acessos (**MEO, pág. 20**), à análise dos riscos de âmbito global, ao relatório anual de segurança e ao programa anual de exercícios (**VODAFONE, pág. 14**).

Entendimento da ANACOM

Tendo em consideração os contributos recebidos, a ANACOM procede à revisão dos prazos previstos no regime transitório aplicável às empresas em atividade à data de entrada em vigor do regulamento, nomeadamente em relação à classificação dos ativos e à elaboração do inventário de ativos, acompanhando a simplificação dos respetivos procedimentos, nos termos agora previstos na subalínea *i)* da alínea *d)* do n.º 2 do artigo 35.º do 2.º Projeto, sem prejuízo da classificação de um conjunto de ativos críticos, nos termos agora previstos na alínea *b)* do mesmo n.º 2.

As disposições específicas relativas à análise dos riscos de âmbito global e ao sistema de controlo de acessos são eliminadas, integrando agora as matérias em causa o âmbito da alínea *d)* do n.º 2 do artigo 35.º do 2.º Projeto, por referência ao disposto nos respetivos Título II e Anexo.

Os prazos para a elaboração do primeiro relatório anual de segurança e para a elaboração e execução do primeiro programa anual de exercícios não são alterados,

por se entender serem os mesmos adequados ao respetivo regime, na sua atual redação, em conformidade com o disposto nas alíneas *e)* e *f)* do n.º 2 do artigo 35.º do 2.º Projeto.

Por último e através do aditamento de um novo n.º 5 ao artigo 35.º do 2.º Projeto, introduz-se a necessária disposição transitória relativamente ao sistema de informação previsto no n.º 2 do artigo 5.º do 2.º Projeto.

5. Conclusão

Considerando as pronúncias recebidas e uma reponderação desta matéria, conclui, assim, a ANACOM pela necessidade de elaborar um segundo projeto de regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas, no qual:

a) Por um lado, procede à alteração da sua abordagem no âmbito da aprovação das medidas técnicas de execução e dos requisitos adicionais, daí resultando uma revisão geral do Título II e a introdução de um novo Anexo; e

b) Por outro lado, procede a revisões específicas dos outros títulos e, em geral, a uma adaptação redatorial do projeto.

Atenta a natureza significativa das alterações em causa, sobretudo no que respeita à nova abordagem no âmbito do Título II e do novo Anexo, entende ainda a ANACOM dever submeter o segundo projeto a um novo procedimento regulamentar e procedimento geral de consulta, nos termos legalmente previstos.