PRONÚNCIA DA

MEO – SERVIÇOS DE COMUNICAÇÕES E MULTIMÉDIA, S.A.

AO

PROJETO DE REGULAMENTO RELATIVO À SEGURANÇA E À INTEGRIDADE DAS REDES E SERVIÇOS DE COMUNICAÇÕES ELETRÓNICAS

VERSÃO NÃO CONFIDENCIAL

03.10.2018

ÍNDICE

NOTA PRÉVIA 2

I. Comentários Gerais 3

II. Comentários Específicos 4

Nota Justificativa 4

Título I – Disposições gerais 6

Artigo 1.º - Objeto 6
Artigo 2.º - Âmbito 6
Artigo 3.º - Definições 8
Artigo 5.º - Meios eletrónicos 8

Título II – Obrigações das empresas em matéria de segurança e integridade 9

Capítulo I – Disposições gerais 9

Artigo 7.º - Medidas técnicas de execução e requisitos adicionais 9

Capítulo II - Medidas específicas 12

Artigo 8.º - Classificação de ativos 12
Artigo 9.º - Inventário de ativos 13
Artigo 10.º - Requisitos da gestão dos riscos 14
Artigo 12.º Exercícios 14
Artigo 13.º Informação aos clientes 15
Artigo 15.º Ponto de contacto permanente 16
Artigo 16.º Equipa de resposta a incidentes de segurança 16
Artigo 17.º Planos de segurança 16
Artigo 19.º Relatório anual de segurança 17

Título III - Obrigações de notificação e de informação ao público 17

Capitulo I - Obrigações de notificação 17

Artigo 21.º Circunstâncias 17
Artigo 22.º Formato e Procedimentos 18

Capítulo II Obrigações de informação ao público 19

Artigo 24.º Conteúdo, meios e prazos de divulgação 19

Título IV – Auditorias à segurança das redes e serviços 20

Capítulo I – Disposições gerais 20

Artigo 28.º Auditorias 20
Artigo 29.º Dever de colaboração 20

Capitulo II – Procedimentos de auditoria 21

Artigo 31.º Fase de pré-auditoria 21
Artigo 32.º Fase de auditoria 21

Titulo V- Disposições finais e transitórias 22

Artigo 35.º Entrada em vigor e disposições transitórias 22

NOTA PRÉVIA

O presente documento constitui a pronúncia da MEO – Serviços de Comunicações e Multimédia, S.A. (doravante "MEO") ao procedimento geral de consulta relativo ao Projeto de Regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas (doravante "Projeto de Regulamento"), aprovado por decisão da ANACOM em 06.07.2018.

Os comentários, sugestões e contributos da MEO apresentados ao longo deste documento tiveram em atenção a atual conjuntura do mercado e o quadro legal existente e não prejudicam a adoção de posições diferentes no futuro, caso se alterem as condições subjacentes à presente pronúncia.

A MEO considera, para todos os efeitos, como **CONFIDENCIAIS** as passagens deste documento devidamente assinaladas como tal, com a indicação de **[IIC]** — Início de Informação Confidencial e **[FIC]** — Fim de Informação Confidencial, uma vez que as mesmas constituem segredo comercial e de negócio, sendo suscetíveis de revelar questões inerentes às atividades e vida interna da empresa.

I. COMENTÁRIOS GERAIS

1. O Projeto de Regulamento aprovado por decisão da ANACOM de 06.07.2018 apresenta alterações significativas face ao primeiro projeto de regulamento publicado em 29.12.2016, grande parte das quais resultou das pronúncias remetidas pelos diversos operadores (e pela APRITEL) no âmbito da consulta pública que decorreu no 1º trimestre de 2017.

2. A MEO congratula a ANACOM pela decisão de adotar um segundo projeto de regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas (SCE), submetendo-o ao presente procedimento geral de consulta, e espera que este novo processo participativo e de auscultação das várias entidades interessadas possa voltar a contribuir decisivamente para melhorar o Regulamento final que será aprovado.

3. A MEO retoma aqui partes da sua pronúncia de 14.03.2017 ao primeiro projeto de regulamento para reforçar que a segurança e integridade das redes de comunicações eletrónicas e a continuidade dos serviços que estas suportam são preocupações primárias dos prestadores de redes e SCE, dada a relevância destas matérias para determinados fatores críticos de sucesso do seu negócio, como sejam a proteção (segurança em sentido estrito) dos seus ativos, a qualidade dos serviços prestados, a confiança e satisfação dos clientes ou a reputação das empresas no mercado.

4. Sem prejuízo de se reconhecer, no entanto, que podem existir objetivos de segurança a nível nacional que extravasam os interesses próprios dos prestadores de redes e SCE, tornando necessária uma intervenção administrativa para impor determinadas medidas, sublinha-se que a escolha e definição destas medidas exige uma ponderação cuidada quanto à sua necessidade, adequação, eficácia e balanço entre os méritos e os custos de implementação, de modo a preservar a proporcionalidade da atuação administrativa.

5. De facto, se, por um lado, a ANACOM goza de uma assinalável liberdade de atuação para decidir se e que medidas deve impor neste campo aos prestadores de redes e SCE, esta circunstância também lhe impõe, em contrapartida, especiais responsabilidades na escolha e justificação dessas decisões.

6. Neste contexto, subsistem no Projeto de Regulamento aspetos que, no entender da MEO, devem ser modificados ou mesmo eliminados por se afigurarem desproporcionais, quer na vertente da sua real necessidade para a prossecução dos objetivos de segurança e integridade a fixar, quer ao nível da intrusão na vida interna e organização das empresas prestadoras de redes e SCE (incluindo no que respeita aos custos de conformação com as medidas).

7. Estes aspetos serão assinalados no capítulo seguinte, de comentários específicos ao Projeto de Regulamento.

II. COMENTÁRIOS ESPECÍFICOS

Nota Justificativa

8. A MEO toma boa nota do reforço da fundamentação do Projeto de Regulamento que a ANACOM incorporou na Nota Justificativa e também no relatório da consulta sobre o primeiro projeto de regulamento.

9. Ainda assim, e como já se deduz dos parágrafos anteriores, a MEO considera que a Nota Justificativa não cumpre devidamente a obrigação de fundamentação do Projeto de Regulamento, em particular no que respeita à necessidade e proporcionalidade das obrigações que o Projeto de Regulamento pretende impor.

10. Na Nota Justificativa pode ler-se que *"Na regulamentação das obrigações das empresas em matéria de segurança e integridade das redes e serviços, foram objeto de ponderação, por um lado, os custos a incorrer pelas empresas no cumprimento das suas obrigações e, por outro, os benefícios daí emergentes, os quais incluem não só a defesa dos interesses dos cidadãos e, em particular, dos utilizadores das redes e serviços, o suporte à continuidade da prestação de serviços relevantes à sociedade e aos cidadãos, a garantia do acesso aos serviços de emergência e, em geral, a promoção do desenvolvimento do mercado interno por via da melhoria da fiabilidade das redes e serviços, como também aqueles resultantes da prevenção de incidentes de segurança e do impedimento ou minimização do respetivo impacto."*

11. Contudo, nem na Nota Justificativa, nem no restante Projeto de Regulamento, são apresentados elementos adicionais que sustentem tal ponderação, aspeto que a MEO volta a criticar de forma veemente, como já havia feito no âmbito do primeiro projeto de regulamento.

12. As implicações organizacionais, processuais, operacionais e financeiras inerentes ao Projeto de Regulamento exigem que a Nota Justificativa não se limite a uma mera declaração de que foram objeto de ponderação os custos e os benefícios das obrigações a impor. É necessário um esforço acrescido de quantificação, senão dos benefícios (cuja natureza pode impossibilitar tal quantificação), pelo menos dos custos de implementação das medidas.

13. Por uma questão de rigor e transparência, é fundamental que se contabilizem os impactos que o Projeto de Regulamento terá sobre os prestadores de redes e SCE. Ainda que a ponderação final sobre a proporcionalidade das medidas não tenha, necessariamente, de ser alterada em função dos custos previstos, nomeadamente nos casos em que a avaliação qualitativa da necessidade e dos benefícios associados às medidas justifica a sua adoção, é importante que estas ponderações sejam claras e com noção dos custos envolvidos.

14. A MEO aproveita esta ocasião, de resto, para reiterar a necessidade da ANACOM incorporar no seu processo de decisão uma prática sistemática e estruturada de Avaliação de Impacto Regulatório (AIR), que discipline a observância de etapas fundamentais do processo regulatório como, desde logo, a caracterização do problema que se pretende resolver, a definição dos objetivos a atingir, a identificação das várias alternativas de atuação e a avaliação dos custos e méritos de cada alternativa que permita justificar a opção final escolhida.[1]

15. De qualquer forma, mesmo não tendo um sistema estruturado de AIR incorporado no seu processo regulatório, faz-se notar que a ANACOM está obrigada a pautar a sua atuação pela observância do princípio da proporcionalidade, que é um princípio basilar do ordenamento jurídico comunitário. Segundo a própria ANACOM[2], citando A. MATTERA: *"Uma dada medida só poderá ser considerada aceitável em face do direito comunitário se por um lado existir um adequado nexo de causalidade entre essa medida e o objetivo legítimo prosseguido, se por outro lado, os meios adotados para atingir tal objetivo deverem ser considerados necessários – isto é, suficientes e não excessivos; e, finalmente, se não houver outras medidas menos severas que, bastando para atingir eficazmente o objetivo visado, comportem menos perturbações do tráfico jurídico-mercantil e sejam, por isso, menos opressivas para os operadores económicos do mercado comum."*

[1] A AIR é uma boa prática regulatória fundamental para a qualidade e robustez do processo regulatório. No âmbito das consultas sobre o plano plurianual da ANACOM, a MEO tem vindo a sugerir ao regulador a adoção desta boa prática, e irá continuar a fazê-lo pois trata-se de uma matéria à qual a MEO atribui a maior relevância.

[2] Sentido Provável de Decisão aprovado a 22.12.2016 sobre a Ponderação da Recomendação da Comissão de 29.11.2016 sobre os processos PT/2016/1888 e PT/2016/1889: acesso local grossista num local fixo e acesso central grossista num local fixo para produtos de grande consumo – justificação fundamentada para não alterar e não retirar o projeto de medida.

16. Assim, no entender da MEO, a fundamentação do Projeto de Regulamento carece de aprofundamento, nomeadamente por via da avaliação quantificada dos custos associados às medidas propostas e da respetiva reponderação face aos benefícios esperados.

17. Enquanto contributo para tal avaliação, e à semelhança do que fez no âmbito do primeiro projeto de regulamento, a MEO procedeu a uma avaliação interna de quais seriam as consequências da implementação das medidas constantes no Projeto de Regulamento **[IIC]** [redacted] **[FIC]**

18. A MEO espera que estes elementos possam ser úteis e tidos em conta na reponderação que, no entender da MEO, a ANACOM deverá fazer de todo o Projeto de Regulamento.

Título I – Disposições gerais

Artigo 1.º - Objeto

19. Por questões de previsibilidade e de proporcionalidade, e não obstante a posição manifestada pela ANACOM no relatório da consulta sobre o primeiro projeto de regulamento, a MEO considera que o Projeto de Regulamento deve especificar claramente quais os SCE abrangidos e cingir a lista àquele conjunto de SCE mais relevantes para os cidadãos e para as empresas, nomeadamente os serviços de voz, dados, incluindo internet, e de TV.

Artigo 2.º - Âmbito

20. A MEO considera o n.º 2 deste artigo excessivo e sugere a sua eliminação. Não se afigura razoável que os prestadores de Redes e SCE fiquem sujeitos a um tal nível de exigência perante a diversidade de fenómenos extremos considerados, alguns dos quais de natureza e intensidades completamente imprevisíveis. Pelo mesmo motivo, a MEO defende também a eliminação da alínea b) do objetivo de segurança número *2 – Segurança física e ambiental*, sendo de assinalar,

[redacted]

de resto, que esta alínea não consta do documento da ENISA de outubro de 2014 "*Technical Guideline on Security Measures - Technical guidance on the security measures in Article 13a*".

21. A MEO defende a eliminação da referência aos equipamentos localizados nas instalações do Cliente que é efetuada no n.º 6 do artigo 2.º, em linha com a posição que expressou no âmbito da consulta sobre o primeiro projeto de regulamento.

22. A razão de ser desta posição é que ainda que a gestão destes equipamentos seja feita pela MEO, não é possível assegurar a este nível o mesmo grau de segurança e integridade que se exige relativamente aos ativos na rede do operador. Em primeiro lugar, existem Clientes que exigem, pese embora a gestão estar confiada à MEO, ter acesso aos equipamentos localizados nas suas instalações. Em segundo lugar, porque estando os equipamentos localizados em instalações do Cliente, o operador não pode garantir a respetiva operacionalidade (por exemplo, o período em que estão energizados) nem que estes não sejam acedidos indevidamente, seja através de ligações físicas, seja através das redes internas do Cliente cujas políticas de segurança o operador não controla.

23. A MEO tomou nota da explicação avançada pela ANACOM no relatório da consulta relativa ao primeiro projeto de regulamento, de que a referência aos equipamentos localizados nas instalações do Cliente está alinhada com o 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, segundo o qual cabe aos prestadores (de serviços de acesso à internet) estabelecer medidas de gestão de 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"*.

24. A MEO faz notar, contudo, que no contexto do Regulamento (UE) 2015/2120 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015, o que está em causa são (apenas) medidas de gestão de tráfego, e não todo o espectro de obrigações previstas no Projeto de Regulamento, como a obrigação de inventariar os ativos, localizá-los com coordenadas geográficas e identificar as entidades detentoras ou gestoras dos locais. Seria de todo desnecessário, inadequado e desproporcional estender este tipo de obrigações aos equipamentos terminais de Cliente.

Artigo 3.º - Definições

25. Não é totalmente evidente a que se refere a palavra "infraestruturas" na alínea a) do n.º 1 (definição de Ativos), e se as mesmas são infraestruturas civis, como edifícios, pelo que se solicita que esta questão seja clarificada.

26. O Projeto de Regulamento não define Ativos Críticos, embora se possa inferir do relatório da consulta sobre o primeiro projeto de regulamento que apenas os ativos de classe A e B são críticos. Contudo, as *Technical Guidelines* da ENISA, e também a própria recomendação do ITU-T X.1057, indiciam que a identificação e a segurança dos ativos deve aplicar-se apenas aos ativos críticos, pelo que se entende que o Projeto de Regulamento deve definir o conceito de Ativos Críticos.

Artigo 5.º - Meios eletrónicos

27. A MEO considera que a referência a "nos termos a determinar pela ANACOM" constante do n.º 1 deste artigo deve ser densificada. A definição dos meios eletrónicos para a troca de informação com a ANACOM no âmbito do Projeto de Regulamento deve ser feita com pelo menos três meses de antecedência face à data de operacionalização desses meios. E caso a sua implementação tenha impacto nos Sistemas de Informação dos prestadores de rede e SCE, a utilização destes meios eletrónicos deve ser previamente acordada com os prestadores.

28. Por outro lado, estando em causa a transmissão de informação sensível, a MEO considera que este artigo deve desde já referir a necessidade de se assegurar a robustez e segurança dos meios eletrónicos a definir para a transmissão, acesso e armazenamento da informação.

29. A MEO mantém que a transmissão e duplicação de informação é, em si mesmo, um fator que potencia riscos de quebra de sigilo, bem como de segurança e integridade das redes e serviços. Neste sentido, a MEO defende que estas trocas de informação devem ser reduzidas ao mínimo indispensável para o bom desempenho das funções da ANACOM neste âmbito, o que significa que determinado tipo de informação, com elevado nível de sensibilidade, não deverá ser transmitida, por meios eletrónicos ou quaisquer outros, podendo em alternativa ficar disponível para consulta por parte de elementos da ANACOM, devidamente credenciados e habilitados, diretamente nas instalações dos operadores.

Título II – Obrigações das empresas em matéria de segurança e integridade

Capítulo I – Disposições gerais

Artigo 7.º - Medidas técnicas de execução e requisitos adicionais

30. A MEO concorda com a abordagem menos prescritiva seguida neste segundo Projeto de Regulamento, mais assente na definição de (25) objetivos de segurança em linha com o documento da ENISA de outubro de 2014 "*Technical Guideline on Security Measures - Technical guidance on the security measures in Article 13a*" que, no entender da MEO, é uma referência chave para este processo.

31. Porém, a MEO opõe-se ao estipulado no n.º 1 do artigo 7º do Projeto de Regulamento, de que as *"empresas devem, nomeadamente, adotar todas as medidas de segurança incluídas nos níveis de sofisticação 1 e 2 para a prossecução de cada um dos 25 objetivos de segurança constantes do Anexo."*

32. Conforme sustentou na resposta à consulta pública sobre o primeiro projeto de regulamento, a MEO defende uma estratégia por etapas para cumprimento dos objetivos definidos ou para elevação do nível de sofisticação das medidas adotadas pelos prestadores, conferindo-lhes tempo e flexibilidade para se adaptarem. Esta é uma estratégia prevista no referido documento da ENISA — ver o ponto *5.3 – Taking a staged approach* para mais detalhes.

33. Sendo certo que o Regulamento irá impor um ónus significativo sobre os prestadores de redes e SCE (questão que o Projeto de Regulamento, como já referido, não dimensiona e que a MEO espera ver corrigida na decisão final sobre esta matéria), é importante que estes custos se possam diluir no âmbito de uma estratégia faseada, sob pena de se poderem constituir como uma barreira à entrada e à expansão de redes e SCE, prejudicando o desenvolvimento do sector.

34. No fundo, uma abordagem passo-a-passo é mais prudente e não coloca em causa o objetivo final que é o de ter, no fim de um determinado período, um nível de sofisticação elevado no cumprimento dos objetivos de segurança definidos.

35. Este é um ponto fulcral do Projeto de Regulamento onde é notória a ausência de uma análise de proporcionalidade com o nível de detalhe que matérias como esta devem exigir, incluindo a comparação de, pelo menos, dois cenários alternativos. Em concreto, importa perceber quais os custos e benefícios associados à exigência do nível 1 e do nível 2, nos termos preconizados

no Projeto de Regulamento (n.º 1 do artigo 7º), num prazo de 18 meses (conforme alínea d), n.º 2, artigo 35º), versus um cenário alternativo em que ao longo de um período de tempo superior (por exemplo, 36 meses, como estava previsto no primeiro projeto de regulamento para as medidas de redundância, robustez e resiliência), se preconize uma evolução gradual (por exemplo, adoção do nível 1 nos primeiros 18 meses e do nível 2 nos segundos 18 meses).

36. A MEO tomou boa nota da fundamentação apresentada pela ANACOM no relatório da consulta sobre o primeiro projeto de regulamento, onde a ANACOM diz *"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"* e que *"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."*

37. Ora, o que a MEO defende é que a *"execução faseada das medidas impostas"* requer um prazo mais alargado que os 18 meses previstos no Projeto de Regulamento, sugerindo-se que, no mínimo, sejam considerados 36 meses, como estava previsto no primeiro projeto de regulamento.

38. Por outro lado, considera-se que a observância do nível de sofisticação que vier a ser adotado não deve ser aferido medida a medida mas sim através de uma média aritmética das várias medidas, já que podem existir situações de objetivos de segurança com implementação de medidas de níveis superiores de sofisticação sem que tenham sido antes implementadas as medidas de níveis de sofisticação inferiores.

39. No que se refere aos requisitos adicionais e às 11 medidas específicas previstas no n.º 3 do artigo 7º, a MEO remete para a posição da APRITEL (que se reproduz de seguida, por facilidade), salientando que algumas destas medidas estão em *overlap* com alguns dos 25 objetivos de segurança definidos no Anexo ao Projeto de Regulamento, conforme tabela seguinte.

Art.	**Medidas específicas**	**Objetivos/medidas de segurança** que correspondem às medidas específicas:
8º	Classificação de ativos	15: Gestão dos ativos 14: Gestão de alterações
9º	Inventário de ativos	
10º	Requisitos da gestão dos riscos	2: Governação e gestão dos riscos

Art.	**Medidas específicas**	**Objetivos/medidas de segurança** que correspondem às medidas específicas:
11º	Procedimentos de Controlo da Gestão Excecional de Tráfego de Acesso à Internet	21: Políticas de monitorização e registo de eventos [parcialmente]
12º	Exercícios	22:Exercícios de planos de contingência
13º	Informação aos clientes	18: Notificação e comunicação de incidentes de segurança
14º	Responsável de segurança	3: Funções e responsabilidades no domínio da segurança [parcial]
15º	Ponto de contacto permanente	3: Funções e responsabilidades no domínio da segurança [parcial]
16º	Equipa de resposta a incidentes	3: Funções e responsabilidades no domínio da segurança [parcial] 16: Procedimentos de gestão de incidentes de segurança [parcial] 17: Capacidade de deteção de incidentes de segurança [parcial]
17º	Plano de segurança	1: Política de segurança 3: Funções e responsabilidades no domínio da segurança 16: Procedimentos de gestão de incidentes de segurança
18º	Deveres específicos de comunicação à ANACOM	3: Funções e responsabilidades no domínio da segurança [parcial]
19º	Relatório Anual de Segurança	16: Procedimentos de gestão de incidentes de segurança [parcial] 22: Exercícios de planos de contingência [parcial]

40. Estes *overlaps* são abordados nos pontos seguintes de análise a cada uma das medidas específicas.

Capítulo II - Medidas específicas

Artigo 8.º - Classificação de ativos

41. Apesar da simplificação face ao primeiro projeto de regulamento, a MEO considera, ainda assim, que a classificação de ativos preconizada no Projeto de Regulamento continua demasiado complexa e exigente, defendendo-se a sua simplificação para um sistema binário, que classifique os ativos em críticos (por exemplo, os que abrangem mais de 500.000 acessos/assinantes) e não críticos, em função da percentagem de parque total de acessos ou assinantes do(s) serviço(s) abrangido(s) e da importância do ativo para o negócio.

42. Assim, a MEO considera que a Classe B deve ser eliminada, até porque o conceito de "impacto negativo grave" que consta da sua definição no n.º 4 do artigo 8.º cria ambiguidade e espaço para interpretações diferenciadas entre os operadores.

43. Na definição de ativos de Classe A, o critério da Área geográfica só deve ser usado no caso do critério relativo ao n.º de assinantes ou acessos afetados ser inaplicável, à semelhança da alínea e), do ponto 3, do artigo 21.º, pelo que a MEO sugere esta adaptação ao n.º 2 do artigo 8.º.

44. No que se refere aos restantes ativos que devem ser classificados na Classe A, não é evidente o significado de "centro principal de gestão e operação" pelo que se solicita a definição deste conceito.

45. A MEO opõe-se à inclusão na Classe A e respetivas obrigações subsequentes dos ativos de que dependa a oferta de redes e serviços através dos quais seja assegurada a continuidade da prestação dos serviços relevantes à sociedade e aos cidadãos, por parte dos "Clientes relevantes" cuja identificação está prevista na al. f) do n.º 2 do artigo 21.º que, por sua vez, remete para o n.º 5 do mesmo artigo.

46. Esta disposição cria ambiguidade, dado o grau de discricionariedade da ANACOM na identificação dos Clientes relevantes e a incerteza quanto ao grau de dependência dos serviços ditos relevantes da oferta de redes e de serviços de comunicações eletrónicas. Além disso, não é de todo razoável que, nos termos da alínea e) do n.º 5 do artigo 21º, a ANACOM possa designar outras entidades, sem que sejam identificados critérios específicos, e com uma antecedência mínima de apenas 5 dias úteis.

47. Além disso, esse tipo de obrigações deverá recair sobre os próprios "Clientes relevantes" a quem deve ser exigido que, no momento da contratação de redes e serviços de comunicações eletrónicas, especifiquem os níveis de serviço que considerem adequados em função da criticidade dos serviços relevantes que prestam à sociedade e do seu grau de dependência das redes e serviços de comunicações eletrónicas. Neste contexto, as obrigações dos fornecedores de redes ou serviços de comunicações eletrónicas devem ser as que ficam contratualizadas no âmbito dos concursos lançados pelos "Clientes relevantes".

48. É de notar que no caso dos Operadores de serviços essenciais, trata-se de empresas que habitualmente estão disseminadas por todo o país, com redes de distribuição à escala nacional. Facilmente se percebe que se os prestadores de rede e SCE tiverem de considerar na Classe A todos os ativos de rede que suportam estes clientes, isso não só é visivelmente desproporcional como desvirtua totalmente a segmentação por criticidade que se pretende implementar.

49. A MEO também não concorda com o disposto na alínea e) do n.º 3 do artigo 8.º, o qual prevê que a ANACOM, no âmbito do planeamento civil de emergência ou de um plano de emergência de proteção civil, possa identificar e impor às Empresas a identificação e classificação de determinados ativos. Com efeito, cabe às Empresas decidir quais os ativos essenciais ou críticos para assegurar o cumprimento dos objetivos e obrigações de segurança que lhes sejam fixados no âmbito invocado pela ANACOM, sendo de todo improvável que terceiras entidades possam estar em melhor posição para tomar, i.e. impor, decisões a este nível de detalhe. As circunstâncias contratuais em que estes ativos estão abrangidos não poderão ser alteradas sem o prévio consentimento da MEO ou acordo entre todas as partes envolvidas.

Artigo 9.º - Inventário de ativos

50. Para além do que decorre dos comentários anteriores relativamente à classificação dos ativos, a MEO considera excessivo o previsto no artigo 9.º quanto ao inventário de ativos. Não se entende a necessidade de se entrar em tais níveis de detalhe relativamente à caracterização dos ativos, questão que deve caber aos prestadores de redes e SCE definir. A MEO sugere que os elementos definidos no ponto 2 deste artigo constituam uma recomendação que os operadores devam levar em linha de conta na elaboração e manutenção do seu inventário de ativos.

51. Por outro lado, enquanto ativos não críticos, não se justifica que os ativos de Classe C façam parte deste inventário, atendendo também ao elevado número de elementos de rede que caem nesta classe e ao esforço que seria necessário para gerir esta lista.

52. Adicionalmente, a MEO opõe-se a que a informação com este nível de detalhe e sensibilidade, mesmo que em formato de síntese, seja enviada à ANACOM, conforme previsto no n.º 5 deste Artigo. Não se percebe, de resto, qual a necessidade da ANACOM em possuir esta informação de todos os operadores e em que medida é que isso contribui para o cumprimento dos objetivos de segurança. As auditorias devem certificar a existência e atualização do inventário e isso é tudo o que a ANACOM deve necessitar de saber.

53. Além disso, conforme já se referiu atrás, a transmissão deste tipo de informação é, em si mesma, uma vulnerabilidade de segurança que deve ser evitada. A MEO propõe que esta disposição seja alterada e passe a prever a obrigação dos prestadores de redes e SCE disponibilizarem esta documentação para consulta, nas suas instalações, a interlocutores da ANACOM devidamente credenciados e habilitados para o efeito, e mediante pedido devidamente fundamentado por parte do regulador.

Artigo 10.º - Requisitos da gestão dos riscos

54. A MEO sugere a eliminação deste artigo que considera redundante com objetivo de segurança número *2 – Governação e gestão de riscos*.

55. Se o propósito da ANACOM é que para este objetivo de segurança seja exigível o nível de sofisticação 3 (Estado da técnica), a MEO considera excessiva a revisão da metodologia e ferramentas de gestão de riscos a cada 2 anos e sugere que esta periodicidade fique ao critério do Operador de acordo com os processos/procedimentos estabelecidos internamente.

Artigo 12.º Exercícios

56. A MEO reitera que deve caber aos prestadores de redes e SCE definir o âmbito e os objetivos do seu plano de exercícios de avaliação de segurança e integridade e salvaguardar que este não motive quaisquer impactos na normal operação das suas redes e serviços.

57. Neste sentido, a abrangência dos exercícios não poderá tomar as proporções descritas no n.º 1 do artigo 12º mas antes deve ser focada em subconjuntos limitados de ativos e de serviços.

58. Quanto à periodicidade máxima, sugere-se que se preveja a possibilidade de, mediante justificação fundamentada, os prestadores de redes e SCE poderem protelar a execução do programa de exercícios e ultrapassar o prazo de 2 anos.

59. Nota-se ainda que a expressão "bianual" presta-se a ambiguidades já que o significado mais comum que lhe é atribuído é o de algo que ocorre duas vezes por ano. Sugere-se, assim, por uma questão de clareza, que a redação do artigo seja revista de modo a tornar inequívoco que a realização dos exercícios deve ocorrer a cada dois anos (e não duas vezes por ano).

Artigo 13.º Informação aos clientes

60. A MEO contesta a necessidade deste artigo e da imposição destas obrigações aos prestadores de redes e SCE. Esta empresa não concorda, de todo, com o entendimento apresentado pela ANACOM no relatório da consulta sobre o primeiro regulamento de que, no que se refere à informação a prestar aos Clientes relevantes, a criticidade dos serviços que estes prestam e o aumento da dependência da prestação desses serviços em relação às redes e SCE em que suportam, justificam que se mantenham e até se reforcem as disposições relativas à sua proteção no Projeto de Regulamento.

61. Sobre esta matéria, a MEO reitera que cabe àquelas entidades identificar o seu grau de dependência das redes e SCE e, em conformidade, contratar junto dos operadores as soluções adequadas de resiliência e os níveis adequados de QoS, incluindo obrigações de comunicação como as que estão previstas no artigo 13º do Projeto de Regulamento.

62. De outro modo, a imposição deste tipo de obrigações aos prestadores de redes e SCE irá criar uma assimetria regulatória, que a MEO considera totalmente injustificada, entre as empresas deste sector e o leque alargado de clientes relevantes, que passará a abranger os operadores de serviços essenciais, proprietários ou operadores de infraestruturas críticas ou qualquer entidade que a ANACOM designe com uma notificação com 5 dias úteis de antecedência.

63. A MEO tomou nota do que a ANACOM refere a propósito das obrigações contratuais de confidencialidade, de que *"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."*, mas assinala que não é, de todo, evidente de que modo é que o envio à ANACOM das comunicações previstas

neste artigo constitui uma *"medida necessária à prossecução das suas atribuições e ao exercício das suas competências."*

Artigo 15.º Ponto de contacto permanente

64. Algumas das situações extraordinárias, previstas nos termos do artigo 2.º, pela sua imprevisibilidade geográfica de ocorrência e magnitude dos efeitos subsequentes, não permitem garantir a exequibilidade das obrigações previstas no n.º 4 deste artigo pelo que a redação deste artigo deverá ser revista em função deste facto e tendo também em consideração a redundância prevista com o Ponto de Contacto Alternativo previsto no n.º 3 deste artigo.

65. As alíneas c) e d) do n.º 1 do artigo 15.º contêm referências à ativação e operacionalização dos procedimentos fixados no âmbito do planeamento civil de emergência e do plano de emergência de proteção civil que suscitam dúvidas quanto à articulação entre as várias entidades envolvidas, aspeto que a MEO solicita seja esclarecido na decisão final sobre o Projeto de Regulamento.

Artigo 16.º Equipa de resposta a incidentes de segurança

66. A MEO considera que o n.º 3 deste artigo deve ser eliminado por configurar uma intrusão excessiva na organização e vida interna dos prestadores de rede e SCE. De facto, estas empresas devem ser livres para escolher a organização e alocação de recursos que considerarem mais adequada. A equipa de resposta a incidentes de segurança prevista neste artigo não deve ter que integrar, necessariamente, o sistema de resposta a incidentes de segurança da informação nos termos a determinar ao abrigo do disposto na alínea d) do n.º 2 do artigo 2.º-A da Lei das Comunicações Eletrónicas.

Artigo 17.º Planos de segurança

67. A MEO considera que este artigo deve ser bastante simplificado, tendo por referência o objetivo de segurança *1 – Política de Segurança*.

68. Sugere-se a eliminação das alíneas b) a d) do n.º 1 uma vez que tratam de matérias já acauteladas pelas medidas previstas nos objetivos de segurança *3 - Funções e responsabilidades no domínio da segurança* e *16 - Procedimentos de gestão de incidentes de segurança*.

Artigo 19.º Relatório anual de segurança

69. A MEO considera que a especificação do relatório anual de segurança constante do artigo 19º do Projeto de Regulamento contém alguns excessos que devem ser eliminados.

70. Em concreto, a MEO sugere que da alínea b) do n.º 1 deve ser retirada a referência aos incidentes sem impacto significativo já que, por definição, este tipo de incidentes não são relevantes e, por outro lado, qualquer tipo de incidente pode ser abrangido, mesmo que a duração tenha sido de poucos segundos e/ou o número de clientes afetados seja residual.

71. Também não se considera razoável a alínea d) do n.º 1 já que o programa de exercícios previsto para o ano civil seguinte pode não estar definido com a antecedência necessária para ser incluído no relatório anual de segurança.

Título III - Obrigações de notificação e de informação ao público

Capitulo I - Obrigações de notificação

Artigo 21.º Circunstâncias

72. A MEO considera que o n.º 2 deste artigo deverá excluir do âmbito do impacto significativo as intervenções planeadas em horário noturno, atendendo a que, tratando-se de intervenções programadas, são, por natureza, alvo de controlo desde o primeiro momento e, por outro lado, o horário noturno limita desde logo o impacto de afetação.

73. No que se refere às obrigações previstas na alínea b) do n.º 2 relativas ao 112 devem ser asseguradas pelo MAI, conforme posição já manifestada pela MEO em sede de resposta à consulta pública de dezembro de 2011.

74. Aliás, a MEO aproveita esta ocasião para detalhar a sua posição nesta matéria: se o Estado considera que há determinadas entidades relativamente às quais é necessário assegurar um grau de proteção especial contra quebras de integridade e segurança no domínio do acesso e serviços de comunicações eletrónicas, para além do que já decorre das obrigações de integridade e se-

gurança, digamos "normais", aplicáveis aos prestadores de redes e SCE e respeitantes à generalidade dos respetivos clientes, o ónus desse grau acrescido de atenção e proteção deve ser colocado diretamente sobre essas entidades e não sobre os prestadores de redes e SCE.

75. Assim, em linha com esta posição, no que se refere à alínea f) do n.º 2, a MEO remete para o comentário efetuado acima no âmbito do artigo 13.º quanto à iniquidade que resultará do facto dos operadores de comunicações eletrónicas passarem a estar sujeitos a obrigações adicionais específicas relacionadas com "Clientes relevantes". As obrigações de comunicar violações de segurança e perdas de integridade que envolvam entidades críticas para a segurança nacional, como a RNSI ou as restantes entidades identificadas, devem ser asseguradas diretamente por estas entidades.

76. A MEO considera, ainda, totalmente inadequado o grau de discricionariedade através do qual a ANACOM pode identificar novos Clientes relevantes, o qual se encontra previsto na alínea e) do n.º 5 deste artigo. A identificação de novos Clientes relevantes deverá ser avaliada previamente com o sector e não pode, em qualquer caso, ficar sujeita a um aviso prévio de apenas cinco dias úteis.

Artigo 22.º Formato e Procedimentos

77. Pelas razões já expostas anteriormente, a MEO não concorda com a introdução da subalínea iv) da alínea f) do n.º 5 deste artigo.

78. Por outro lado, considera-se que não deve ser requerida a indicação das freguesias e dos concelhos na notificação de fim de impacto significativo (alínea c) do n.º 7 deste artigo). A recolha e preparação desta informação implica custos significativos em termos de Sistemas de Informação (SI), que não se justificam face ao valor acrescido da informação. É de notar que, dependendo do incidente, este requisito pode dar origem a uma listagem de elevada dimensão, além de que para certos serviços a afetação de uma dada freguesia pode ser parcial. O apuramento concreto das freguesias e respetivos concelhos é um processo complexo e moroso, particularmente quando são afetados determinados segmentos de rede ou tecnologias, pelo que a indicação concreta das zonas afetadas deverá ser limitada à notificação final.

79. Adicionalmente, a MEO considera que não é justificável incluir na notificação de fim a descrição da situação do impacto existente no momento do fim de impacto significativo (alínea d) do n.º 7), admitindo, ainda assim, que em alguns casos, embora pontuais, esta informação possa ter

alguma relevância. O mesmo é aplicável no que respeita à alínea k) do n.º 9 deste artigo, relativamente à notificação final.

80. Por fim, atendendo à sua experiência nesta matérias e aos tipos de incidente que se têm vindo a verificar desde a entrada em vigor da Deliberação de 12.12.2013, a MEO considera que no n.º 11 deste artigo devem ser incluídas as causas raiz "Equipamento de Cliente" e "Intervenção Planeada". A MEO não concorda com o entendimento da ANACOM, expresso no relatório da consulta sobre o primeiro projeto de regulamento, de *"manter o alinhamento, nesta matéria, com a documentação da ENISA e não se constatar necessidade de adaptação resultante de alguma característica especial do país",* pois a prática demonstrou que estas causas específicas não são mapeáveis nas causas definidas na documentação da ENISA.

81. A MEO considera também que deve ser eliminada a obrigatoriedade do contacto telefónico dado que o envio do e-mail já é, por si só, suficiente. Adicionalmente, após a receção da notificação inicial e/ou de fim, a ANACOM deve enviar um aviso de receção para a empresa, no qual inclua a identificação do n.º da violação de segurança ou perda de integridade (i.e. ID-R-NOT).

Capítulo II Obrigações de informação ao público

Artigo 24.º Conteúdo, meios e prazos de divulgação

82. A MEO contesta o aumento do nível de exigência preconizado no Projeto de Regulamento no que respeita ao conteúdo, meios e prazos de divulgação de informação ao público sobre incidentes de quebra de integridade e segurança de redes e SCE.

83. O prazo máximo de uma hora previsto na alínea c) do n.º 1 deste artigo é demasiado exigente e pode ter como inconveniente ocupar com atividades de reporte recursos que deviam estar prioritariamente focados em ações de mitigação e resolução dos incidentes. Adicionalmente, obriga a ter recursos especializados na publicação de informação e na comunicação com o Cliente permanentemente disponíveis (24 x 7), o que não se afigura de todo proporcional. Também não se percebe os fundamentos para esta alteração proposta pela ANACOM, atendendo a que esta questão já tinha sido equacionada no SPD de 22.12.2011 relativo às notificações por violação da integridade e segurança das redes e SCE e, entretanto, em virtude dos comentários expostos pelos operadores no processo de consulta pública, a ideia não prosseguiu.

84. Sobre este ponto, importa, igualmente, salientar que, sem prejuízo do direito de os Clientes/utilizadores terem conhecimento sobre as situações, este não deverá ser um dos pontos centrais do regulamento, sobretudo porque não se vislumbra em que medida é que os Clientes/utilizadores possam ser prejudicados com o facto de as comunicações serem efetuadas/contabilizadas apenas em horas úteis.

85. A obrigação prevista na subalínea ii) da alínea a) do n.º 1, de apresentar informação desagregada ao nível da freguesia, também se afigura excessiva e desproporcional, já que para além de ser complexa de obter implica desenvolvimentos de SI. A MEO considera que esta obrigação deve ser eliminada ou, pelo menos, ser transformada em recomendação.

Título IV – Auditorias à segurança das redes e serviços

Capítulo I – Disposições gerais

Artigo 28.º Auditorias

86. No que se refere ao n.º 2 deste artigo, tem de ser ponderada a relativamente reduzida dimensão do mercado e a existência no mercado de empresas auditoras com o nível de experiência indicado.

87. A rotatividade de escolha das empresas auditoras prevista no n.º 3 deste artigo deve ser uma recomendação (em vez de imposição), de modo a minimizar os constrangimentos na seleção de empresas auditoras que cumpram os requisitos estabelecidos. Sugere-se que a rotatividade seja exigida ao nível das equipas envolvidas nos processos de auditoria, não das empresas auditoras.

88. Note-se que a rotatividade das empresas auditoras também tem o inconveniente de informação estratégica e confidencial passar a ser objeto de conhecimento de um leque alargado de auditores/consultores, o que potencia riscos de violação de segurança para os prestadores de redes e SCE.

Artigo 29.º Dever de colaboração

89. No que se refere ao n.º 2 do artigo 29.º, por um lado, a MEO considera que os colaboradores da ANACOM que estejam envolvidos nestes processos devem também ficar sujeitos a critérios de

exigência como os aplicáveis às empresas auditoras e seus colaboradores, como seja a credenciação adequada emitida por entidades competentes para acesso a matéria classificada.

90. Por outro lado, o acesso, por parte da ANACOM, às auditoras e aos fornecedores e colaboradores relevantes deve ser feito por intermédio do próprio prestador de redes e SCE e deverá acontecer apenas e só quando existam sérias e fundamentadas dúvidas sobre os resultados da auditoria.

Capitulo II – Procedimentos de auditoria

Artigo 31.º Fase de pré-auditoria

91. A MEO defende a eliminação deste artigo uma vez que se afigura excessivo, desnecessário e inadequado sujeitar a aprovação da proposta de auditoria (preparada em conjunto com a empresa auditora) a uma avaliação da ANACOM, quando não se reconhecem nem são conhecidas na ANACOM competências específicas para este efeito.

92. Sem conceder, a manter-se a necessidade de apresentar à ANACOM uma proposta de auditoria, a MEO considera que nesta fase de pré-auditoria não se justifica apresentar mais do que o Plano de Auditoria, conforme descrito na alínea f) do n.º 1, pelo que as restantes alíneas a) a e) do n.º 1 devem ser eliminadas, e que a proposta não deve ficar pendente de aprovação por parte da ANACOM.

93. Ainda sem conceder, a MEO considera que a apresentação de propostas de auditorias a cada dois anos, conforme previsto na alínea b) do n.º 2 deste artigo não se justifica, devendo antes ficar previsto um prazo de cinco anos.

Artigo 32.º Fase de auditoria

94. Na sequência dos comentários anteriores, a MEO contesta o n.º 1 deste artigo e sugere a sua eliminação.

Titulo V- Disposições finais e transitórias

Artigo 35.º Entrada em vigor e disposições transitórias

95. A MEO não compreende a alteração preconizada pela ANACOM no Projeto de Regulamento relativamente ao prazo para adotar os procedimentos de controlo da gestão excecional de tráfego de acesso à Internet, nos termos previstos no artigo 11.º do Projeto de Regulamento, definindo agora 80 dias úteis (alínea c) do n.º 2 deste artigo) quando este prazo era de 18 meses no primeiro projeto de regulamento.

96. A MEO contesta esta alteração e faz notar que esta medida exige desenvolvimentos de SI, podendo ter de envolver fornecedores, o que não é possível de realizar em 80 dias. Assim, defende-se que este prazo seja fixado em 18 meses, conforme constava do primeiro projeto de regulamento.

97. Por fim, em linha com os comentários anteriores ao *Artigo 7.º - Medidas técnicas de execução e requisitos adicionais*, a MEO defende que o prazo de 18 meses definido no Projeto de Regulamento na alínea d) do n.º 2 deste artigo para adotar *"as restantes medidas de segurança aplicáveis nos termos previstos no Título II e no Anexo ao presente regulamento, sem prejuízo do disposto nos n.os 3 e 5 do presente artigo"* deve ser alargado para 36 meses.