[redacted]

From: [redacted]@nos.pt>
Sent: 14 de março de 2017 18:09
To: regulamento.seguranca@anacom.pt
Cc: [redacted]
Subject: Resposta do Grupo NOS à Consulta sobre projeto de regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas
Attachments: Comentários NOS - Regulamento de Segurança (14032017).pdf

Exmos. Senhores,

Junto se envia a resposta do grupo NOS (NOS Comunicações, S.A., NOS Açores Comunicações, S.A. e NOS Madeira Comunicações, S.A) à consulta sobre projeto de regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas.

A resposta em anexo não contém elementos classificados como confidenciais.

Disponível para qualquer esclarecimento adicional,

Cumprimentos,

[redacted]
NOS Comunicações, S.A
Rua Ator António Silva, nº9
Campo Grande, 1600-404 Lisboa

Consulta sobre o projeto de regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas

Comentários da NOS

Versão não confidencial

14 de março de 2017

Índice

1. Sumário Executivo

A NOS confere primordial relevância segurança e integridade das suas redes e serviços de comunicações eletrónicas, fatores determinantes para a confiança dos utilizadores e do mercado em geral nos seus serviços. Neste seguimento, a NOS tem interesse e atua proactivamente na minimização de potenciais incidentes que afetem a segurança e integridade das suas redes, seguindo e adotando as melhores práticas nesta matéria.

Face ao seu interesse, envolvimento e conhecimentos adquiridos no âmbito da segurança e integridade das redes e serviços a NOS reconhece o mérito das propostas apresentadas pela ANACOM no documento em consulta, nomeadamente a devida e exaustiva identificação dos diferentes níveis de atuação para endereçar o tema da segurança e integridade. Reconhece-se que proposta da ANACOM constitui um "guião" válido e útil para definir as ações a desenvolver, em particular, por operadores que estejam a iniciar a sua atividade e como tal não tenham ainda desenvolvido os seus próprios processos.

Porém, não é o caso da NOS, como não será de outros operadores nacionais, que ao longo do tempo têm vindo a desenvolver e a aperfeiçoar os seus processos e procedimentos tendentes à segurança e integridade das suas redes e serviços. É convicção da NOS que tal é do conhecimento da ANACOM. Foi, por isso, com alguma surpresa que a NOS constatou que a ANACOM propõe no Projeto de Regulamento medidas muito restritivas, exigentes e ambiciosas desconsiderando os procedimentos já implementados e sem que tenha apresentado os resultados de uma análise, designadamente do risco do país em geral e dos operadores nacionais, em particular, que justifique uma abordagem tão mais prescritiva e exigente do que a adotada por outros suas congéneres cujos países apresentam, à partida, um risco superior ao nacional.

A fundamentação apresentada é ainda limitada pela ausência de uma avaliação de impacto na qual a ANACOM concretize o racional para a imposição das medidas propostas considerando os respetivos custos *vis-à-vis* os benefícios.

Neste seguimento, a NOS sugere uma abordagem alternativa assente na definição de objetivos de segurança, a qual apresenta claras vantagens do ponto de vista da flexibilidade, proporcionalidade, adaptabilidade e eficiência, sem colocar em causa as preocupações que, no entender da NOS, motivam a proposta da ANACOM.

A NOS entende que esta abordagem alternativa deverá ter como referência os objetivos de segurança (SO)[1] descritos pela ENISA nas suas *Technical Guidelines for Minimum Security Measures*, salientando-se que esta abordagem foi adotada por reguladores de referência como o OFCOM e a COMREG e, como referido pela própria ENISA, não põe em causa a comparabilidade entre operadores e aferição de cumprimento das obrigações impostas.

[1] SO: security objetives

Para concretizar esta abordagem alternativa assente na definição de objetivos de segurança, a NOS sugere que a ANACOM promova um grupo de trabalho conjunto com os operadores para efetuar a adaptação do Projeto de Regulamento agora em análise, sendo que a NOS apresenta neste documento uma ilustração daquele que poderá ser o exercício da referida adaptação.

Caso a ANACOM decida não optar por esta abordagem alternativa focada nos objetivos de segurança, o Projeto de Regulamento terá, no mínimo, que ser alvo de ajustamentos no sentido de o tornar menos prescritivo e mais razoável face ao enquadramento comunitário e nacional.

Deverá ser claro que o âmbito do futuro Regulamento está limitado à vertente de segurança relativa à interrupção e continuidade dos serviços, assim como aos serviços de comunicações eletrónicas relevantes, tal como tem sucedido até ao momento com o mecanismo de notificação de incidentes de segurança com impacto significativo.

A classificação de ativos deverá ser simplificada, designadamente diminuindo o número de classes relevantes. Também o processo de inventário de ativos deverá ser alvo de ajustamentos, incluindo os prazos e abrangência de revisão, os quais a NOS considera serem demasiado frequentes e exigentes. E deverá ser eliminada qualquer obrigação de comunicação de informação sobre ativos à ANACOM ou a entidades por ela devidamente credenciadas para minimizar o risco de fuga de informação, mesmo que inadvertida. O cumprimento dos objetivos que se pretendem atingir com tal envio é assegurado pela disponibilidade da informação para consulta pela ANACOM e por outras entidades em sua representação devidamente credenciadas, nas instalações dos operadores e no seguimento de pedido prévio.

A NOS propõe ainda a revisão do processo de análise de riscos, de modo a focá-lo nos ativos sujeitos a riscos e ameaças que afetem a segurança e a integridade das redes e serviços.

Por sua vez as medidas de resiliência, de robustez e redundância terão de ser alteradas no sentido de garantir a sua exequibilidade, nomeadamente no que respeita à redundância em locais geográficos distintos, bem assim torná-las mais proporcionais. Para este efeito, a NOS entende que deverão, nomeadamente, ser estabelecidos objetivos a atingir para determinados ativos em função da sua criticidade e devem ser evitadas medidas tão prescritivas como as propostas pela ANACOM, como é, por exemplo, o caso da autonomia dos sistemas alternativos de energia.

No que respeita a testes, reconhecendo-se a sua importância, a NOS entende que a sua realização com uma regularidade e âmbito tão abrangente como a refletida no Projeto de Regulamento pode ter efeitos contraproducentes, na medida em que existe risco da sua realização ter impacto na continuidade da prestação dos serviços.

Quanto ao procedimento de auditorias, a NOS salienta que as mesmas devem ser efetuadas de acordo com um ciclo de melhoria contínua, tendo em máxima consideração a razoabilidade dos investimentos necessários para resolver as Não-Conformidades, cuja

resolução deve ser focada nos objetivos a alcançar e não na forma concreta de alcançar estes objetivos. Ainda no âmbito das auditorias, sem prejuízo do dever de colaboração, a NOS defende que qualquer contacto com os fornecedores relevantes ao nível da segurança e integridade das redes e serviços deve ser efetuado pelos e/ou com conhecimento e participação dos operadores.

Por último, a NOS defende que o futuro Regulamento preveja expressamente a opção de empresas que integram o mesmo Grupo deem cumprimento às obrigações aí previstas individualmente ou de forma integrada, de modo a garantir maior eficiência acautelando situações em que tais empresas na sua atividade normal já tenham processos integrados ou partilhados.

1. Introdução

A NOS Comunicações, S.A., NOS Açores Comunicações, S.A. e NOS Madeira Comunicações, S.A., doravante conjuntamente designadas por "NOS", vêm pelo presente documento apresentar os seus comentários ao projeto de regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas ("Projeto de Regulamento").

No capítulo 2 serão apresentados comentários gerais e no capítulo 3 a NOS expõe os seus comentários específicos. No âmbito destes últimos sugere-se e exemplifica-se uma abordagem alternativa à seguida no Projeto de Regulamento para perseguir os fins que este, no entender da NOS, visa alcançar. Em concreto, sugere-se que o futuro Regulamento defina os objetivos a atingir tendo como referência o documento *Technical Guidelines on Security Measures*, versão de outubro de 2014, da ENISA, deixando ao critério dos destinatários a definição dos processos e medidas concretas a adotar. Sem prejuízo da sugestão de uma abordagem alternativa e respetiva exemplificação, no âmbito dos comentários específicos a NOS apresentará também sugestões de alteração ao Projeto de Regulamento mantendo a abordagem adotada pela ANACOM na sua proposta.

2. Comentários gerais

2.1. Adequação das medidas: comparação internacional

O Projeto de Regulamento em análise surge enquadrado pelos artigos 13.º-A e 13.º B da Diretiva n.º 2002/21/CE, do Parlamento Europeu e do Conselho, de 7 de março de 2002[2], o qual é comum a todos os Estados membros da União. Neste seguimento e atento o objetivo de promoção do mercado interno, a definição pela ANACOM das medidas técnicas e operacionais relativas à segurança e integridade das redes não pode deixar de ter em conta o modo como outros reguladores comunitários atuaram neste âmbito, sem prejuízo da necessidade de acautelarem as especificidades de cada Estado Membro.

Ora, realizado um exercício comparativo das medidas técnicas e operacionais relativas à segurança e integridade das redes definidas por outros reguladores europeus no âmbito da regulamentação dos referidos artigos 13.º-A e 13.º-B, conclui-se que a ANACOM adotou a abordagem mais ambiciosa, não se antecipando motivos para tal, pelo contrário.

De facto, em resultado do *benchmark* efetuado pela NOS foi possível constatar que, de entre o grupo de países analisados[3], as propostas apresentadas pela ANACOM consubstanciam o regime mais exigente e abrangente. Nem mesmo o regulador sueco (PTS), cujas obrigações são aquelas que mais se aproximam do regime preconizado pela

[2] Diretiva relativa a um quadro regulamentar comum para as redes e serviços de comunicações eletrónicas, na sua redação em vigor
[3] Reino Unido, Irlanda, Espanha, França, Bélgica, Suécia, Itália e Grécia

ANACOM, apresenta prazos de implementação e obrigações de reporte tão exigentes como a ANACOM.

A NOS não acredita que os riscos de segurança e integridade dos serviços de comunicações eletrónicas em Portugal sejam superiores aos dos países incluídos no *benchmark*. Aliás, tendo em conta apenas os aspetos gerais a nível geopolítico, natural e social os países em causa apresentam maior suscetibilidade a incidentes do que Portugal.

Reguladores de referência como o OFCOM[4] ou a COMREG[5] optaram pela publicação de linhas de orientação sobre as obrigações em matéria de segurança e integridade de redes, nas quais definem um conjunto de objetivos a serem alcançados pelos operadores, garantindo porém flexibilidade na definição das medidas a serem adotadas para alcançar estes fins.

Salienta-se que quer na adoção dos requisitos mínimos de segurança pelos operadores, quer na aferição do seu cumprimento, o OFCOM e a COMREG recomendam que seja tida em máxima consideração as linhas de orientação da ENISA:

(...) We consider that the ENISA Technical Guideline on Security Measures sets out good practice which needs to be considered to ensure compliance with section 105A(1) (...) [6]

(...) Ofcom's view of relevant issues will be informed by ENISA's Technical Guideline on Security Measures. This document was developed as a guide for use by regulators when assessing compliance with the European Directive from which section 105A is drawn. (...)[7]

(…) Operators should familiarise themselves with ENISA guidelines for Minimum Security Measures. ComReg will consider the guidelines in this document as well as other specific circumstances when assessing an Operator's compliance with its obligations (...) [8]

Aliás, o regulador irlandês admite mesmo a possibilidade de serem propostos pelos operadores *standards* alternativos aos apresentados pela ENISA, desde que estes cumpram com os objetivos estabelecidos.[9]

Tal como já explicitado anteriormente, a NOS entende que a abordagem seguida pelo OFCOM e COMReg resulta em claros benefícios, porquanto confere aos operadores flexibilidade para definirem as medidas que consideram mais adequadas para endereçar os objetivos estipulados atenta a sua realidade, evitando-se a imposição de soluções *one size fits all* que podem revelar-se contraproducentes, desajustadas ou mesmo inexequíveis, tal como salientado pela ENISA.

[4] Ofcom guidance on security requirements in sections 105A to D of the Communications Act 2003
[5] Comreg Reporting & Guidance on Incident Reporting & Minimum Security Standards
[6] Ofcom guidance on security requirements in sections 105A to D of the Communications Act 2003, ponto 3.14, p. 4
[7] Idem, ponto 3.5, p. 6
[8] Comreg Reporting & Guidance on Incident Reporting & Minimum Security Standards, p. 40
[9] Idem, ponto 127, p. 40

Adicionalmente, e muito relevante para a situação de operadores como a NOS, tal abordagem permite compatibilizar o desenvolvimento normal da sua atividade comercial com os objetivos regulatórios, dispensando a duplicação de esforços e recursos, a qual é totalmente ineficiente e deve ser minimizada em qualquer caso, e mais ainda num contexto (que se vive há vários anos e que não dá sinais de se alterar) de grande pressão do ponto de vista de receitas e custos do setor, como também já referido.

Face ao exposto, partindo das propostas apresentadas pela ANACOM no Projeto de Regulamento no capítulo relativo aos comentários específicos apresenta-se um exercício ilustrativo do modo como poderá ser concretizada uma abordagem semelhante à prosseguida pelos reguladores britânico e irlandês, tendo como referência as referidas linhas de orientação emitidas pela ENISA.

2.2. A abordagem adotada é excessiva e demasiado prescritiva (restritiva)

Como é do conhecimento da ANACOM, a segurança e integridade das redes e serviços de comunicações eletrónicas assume grande importância para os operadores, incluindo para a NOS. Pois, a segurança e integridade das redes assume-se como um fator decisivo para a confiança que os atuais e potenciais clientes depositam nos nossos serviços e é um aspeto muito relevante na escolha de um prestador de comunicações para o mercado.

Dado este contexto e desde logo pelo interesse estritamente comercial de aumento de clientes - na verdade o interesse extravasa o mero interesse comercial - a NOS tem canalizado avultados recursos para garantir um elevado nível de segurança e integridade da sua rede e dos seus serviços. Neste momento a NOS dispõe de processos e ferramentas robustas que visam garantir a segurança e integridade da sua rede e serviços e as quais se pretende permanentemente melhorar para acompanhar a evolução tecnológica e de mercado e aumentar a robustez e resiliência da rede e serviços da NOS e assim garantir a confiança nos nossos serviços, condição (cada vez mais) essencial para angariação e manutenção de clientes.

Com efeito, a NOS adota as melhores práticas de gestão dos riscos associados à segurança e continuidade, tendo vindo a desenvolver, desde a década de 2000, os seus programas de Gestão da Segurança da Informação (ISM - Information Security Management) e de Gestão da Continuidade de Negócio (BCM - Business Continuity Management).

A Política de Segurança da NOS define os Princípios de Segurança da Informação que deverão ser seguidos pelos colaboradores e prestadores de serviço da NOS, bem como define os níveis e os domínios de segurança e os respetivos objetivos de controlo. A Política, que visa a proteção da informação e ativos, baseia-se voluntariamente na adaptação de *standards* internacionais recomendados, tais como a norma ISO 27001 e as

Technical Guidelines for Security Measures da ENISA - European Network and Information Security Agency[10].

A NOS possui processos específicos para garantir a Continuidade das operações críticas e dos serviços de comunicações prestados aos seus Clientes, incluindo também Planos de Gestão de Crise para cenários de falhas técnico-operacionais ou outros com impacto nos Clientes e na reputação da marca e está continuamente a melhorar estes processo e procedimentos no sentido de garantir maior robustez e resiliência dos serviços que disponibiliza.

A NOS está certificada na norma ISO 27001 - Sistema de Gestão da Segurança da Informação (Information Security Management System – ISMS).

Face ao seu interesse, empenho e experiência ao nível de segurança e integridade das redes e serviços de comunicações eletrónicas, a NOS reconhece que o Projeto de Regulamento apresentado pela ANACOM constitui um bom "manual de operações" neste domínio e que poderá ser tido como referência por uma entidade que pretenda iniciar atividade no setor para identificar os aspetos que deve ter em conta relativamente à segurança e integridade da respetiva rede e serviços.

Sucede que, conforme atrás se aludiu, a NOS (e acreditamos outros operadores presentes no mercado), dispõe já de ferramentas e processos para atingir os objetivos que o Projeto de Regulamento visa alcançar. Pelo que, encerrando o referido projeto uma abordagem altamente prescritiva e detalhada quanto ao modo de atingir os objetivos, o cumprimento do mesmo implica um esforço adicional que não é razoável, nem eficiente do ponto de vista social. Pois, a adoção do Projeto de Regulamento na sua versão atual implicará em alguns casos o estabelecimento de processos/procedimentos paralelos para atingir o mesmo fim e, noutros, impõe procedimentos que efetivamente não se consideram proporcionais, nomeadamente atenta a realidade de Portugal e do operador em causa.

Adicionalmente, não se escamoteia, no âmbito das propostas concretas de medidas e procedimentos para atingir determinados fins, a ANACOM é excessiva na abrangência de determinadas medidas e na repetição de determinados exercícios face aos riscos existentes e aos objetivos que se pretendem atingir. Referimo-nos, por exemplo, ao âmbito do inventário ou à frequência e âmbito da revisão das análises de risco.

Face ao exposto, a NOS defende que a ANACOM proceda à alteração do projeto de Regulamento no sentido de seguir uma abordagem assente na fixação dos objetivos de segurança a alcançar, deixando aos operadores a definição das medidas e processos concretos a seguir para os atingir. A NOS sugere que os objetivos de segurança sejam

[10] Política Geral de Segurança da NOS disponível em: http://www.nos.pt/institucional/PT/sobre-a-nos/quem-somos/Documents/NOS-PSI%20-%20Politica%20Geral%20de%20Seguranca%20da%20Informacao_v1.0_vP.pdf

estabelecidos tendo como referência as *Technical Guidelines on Security Measures* da ENISA, elaboradas especificamente para o setor das comunicações eletrónicas, tendo sido previamente discutidas pelos *stakeholders* relevantes a nível europeu.

No âmbito dos comentários específicos, a NOS irá apresentar uma demonstração de um possível exercício de mapeamento do conteúdo do Projeto de Regulamento com os objetivos de segurança incluídos no documento da ENISA e o modo como estes podem ser usados como referência para a elaboração do futuro Regulamento.

A propósito das *Technical Guidelines on Security Measures* de salientar que, embora a ENISA reconheça no documento que uma abordagem assente na imposição de medidas específicas pode conferir maior previsibilidade, destaca que "*in most settings the sector, the organizations involved, the technology used, is just too diverse to allow for a single checklist of minimum security measures for the entire sector. Often only very high-level security standards could be reasonably applied to a wider number of organizations.*"[11]

Mais importante, a ENISA salienta que a imposição de medidas prescritivas pode ser contraproducente, atendendo ao dinamismo e mudanças constantes a que o setor está sujeito, sugerindo que em alternativa a esta abordagem seja conferido aos OPS a possibilidade de proactivamente adotarem as medidas que consideram adequadas para endereçar os riscos de segurança identificados:

(...) This makes it hard to capture the high-level security requirement of Article 13a comprehensively in a list of detailed security measures. In this light, NRAs should focus first on supervising that providers assess risks and proactively take appropriate security measures, rather than on trying to cast detailed security measures in stone (...). [12]

Note-se que a abordagem baseada na fixação de objetivos que acaba de se propor não coloca em causa a comparabilidade de cumprimento do Regulamento a aprovar, na medida em que a aferição de tal cumprimento poderá ser feita via *self assessment* ou através de auditorias externas, incluindo auditorias promovidas pela Autoridade Reguladora. Acrescente-se a este propósito que a obtenção de certificação em determinada Norma não é feita, em geral, em contrapartida do seguimento de processos/medidas específicos (as) pré-definidos (as), mas antes através da demonstração de atingimento de determinados objetivos de controlo fixados na norma em causa. Também a ENISA no seu documento *Technical Guidelines on Security Measures* refere o *self-assessment* como forma de aferir o cumprimento pelo mercado (capítulo 5.2) acrescentando também a possibilidade de realização de diferentes tipos de auditoria.

2.3. A proposta carece de fundamentação

No seguimento do exposto nos pontos anteriores, a NOS entende que a ANACOM não logrou justificar cabalmente, através de uma análise custo-benefício, o nível e detalhe das

[11] ENISA, Technical guidance on the security measures in Article 13a, p. 26
[12] Idem, p. 28

medidas incluídas no Projeto de Regulamento. Regista-se que a ANACOM refere no ponto 7. da nota justificativa 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 impacte.*

Todavia, a ANACOM não apresenta qualquer informação concreta sobre os custos e benefícios de implementação das medidas que propõe tomando em conta os procedimentos já adotados pelos operadores e o risco geral e específico de Portugal neste domínio.

Na realidade nada é referido quanto ao custo da adaptação de procedimentos atuais ou adoção de processos adicionais pelos operadores nacionais face ao que já está implementado[13], nem aos problemas e riscos concretos identificados pela ANACOM que justificam o âmbito, nível e detalhe de medidas propostas que, em geral, são mais ambiciosas do que as adotadas por reguladores de outros Estados Membros, como detalharemos no ponto seguinte, em prejuízo (ónus adicional) dos operadores nacionais e em detrimento do mercado interno.

Neste seguimento não é demais relembrar que as empresas do setor continuam altamente pressionadas ao nível de crescimento de receitas e que o mercado de capitais, apesar de todo o percurso que tem sido feito nos últimos anos, continua a exercer um enorme escrutínio sobre a evolução dos custos das empresas do setor e continua a reclamar a sua diminuição, penalizando o aumento de investimentos e gastos.

Ora, de acordo com a análise da NOS, a implementação das medidas propostas pela ANACOM acarreta alterações significativas às ferramentas corporativas afetas à gestão da rede e implica um esforço muito elevado a nível processual, bem como em termos de alocação de recursos dedicados à transformação e, o qual não se pode dissociar do contexto dos mercados financeiros que acabou de se descrever e porque se entende que as medidas propostas são desproporcionais e injustificadas face aos riscos do país, às medidas implementadas proactivamente pelos operadores, bem como em comparação com o tipo de medidas impostas por outros Estados Membros da União.

[13] Ainda que não tenha sido entretanto solicitada uma atualização, recorda-se que em 2012 a ANACOM solicitou informação aos operadores para aferir o seu grau de cumprimento de objetivos de segurança e não houve qualquer continuidade/consequência ou relacionamento das medidas propostas relativamente ao levantamento feito anteriormente.

Enquanto defensor do interesse dos cidadãos e do desenvolvimento sustentável do setor, o que implica necessariamente uma visão de médio e longo prazo, o regulador não pode descurar esta realidade nas suas tomadas de decisão.

O Código de Procedimento Administrativo [14], mais concretamente no artigo 99.°, prescreve e exige que o Projeto de Regulamento seja acompanhado da respetiva nota justificativa, isto é, da fundamentação específica para as soluções adotadas no projeto de regulamento.

Esta fundamentação deve ser jurídica, no sentido de aludir às normas legais que habilitam e servem de base à emissão do regulamento, mas não se pode ficar por aí. Com efeito, deve ainda incluir a chamada fundamentação administrativa, ou seja, a menção aos concretos interesses públicos implicados cada uma das soluções, de tal forma que possa resultar claro para os interessados a ponderação entre custos e benefícios. Esta segunda vertente da fundamentação é a única que possibilita o controlo da oportunidade, do mérito e da adequação das soluções normativas propostas no projeto de Regulamento.

Pois bem, a ANACOM, pelo trecho supra transcrito, procede efetivamente à enunciação qualitativa de alguns interesses implicados, mas não se deteta nem identifica nesse desfiar, de certo modo generalista e vago, uma quantificação concreta dos custos.

Exatamente o mesmo acontece relativamente aos supostos benefícios que, sendo mais ou menos nomeados, não são igualmente monetizados ou quantificados.

Ora, tal revela-se de capital importância para se poder aquilatar com rigor da bondade ou não das soluções propostas e que de outra forma se aproximam não de análises reais mas de proclamações[15].

No seguimento do exposto, a NOS solicita que a ANACOM realize e disponibilize um exercício de *impact assessement* das medidas propostas no âmbito do qual sejam ponderados os impactos administrativos, operacionais e financeiros face aos benefícios que a ANACOM pretende atingir.

Neste âmbito, devem ser indicados os riscos e problemas identificados e que justificam o grau de intervenção adotado. Apenas desta forma será possível garantir que a intervenção não descura os princípios de razoabilidade e proporcionalidade, assim como é eficiente na resolução dos riscos e ameaças identificados, permitindo defender o interesse dos cidadãos e do desenvolvimento sustentável do setor no médio e longo prazo. A NOS está

[14] Decreto-Lei n°4/2015

[15] A pertinência, diríamos até essencialidade, da nota justificativa com o grau de exigência referido faz que, diversa da melhor doutrina especializada na matéria defenda que a sua falta ou insuficiência seja geradora da invalidade do regulamento final, por vício de procedimento. Ver Mário Esteves Oliveira, Pedro Gonçalves, João Pacheco de Amorim, in Código de Procedimento Administrativo Anotado, pág. 522, vide, comentário V ao artigo 116.°, 2.a edição, Almedina, Coimbra, 1997). Dir-se-á, de resto e até, que a ausência da nota justificativa ou a sua não completude nos termos mencionados impede a adequada pronúncia e participação dos interessados acerca das soluções normativas escolhidas e das razões para a sua escolha, participação essa que configura o exercício de um direito fundamental por parte dos interessados

certa que tal exercício concluirá pela necessidade de adaptação do Projeto de Regulamento.

2.4. Cumprimento do regulamento por empresas do mesmo grupo

O Projeto de Regulamento é omisso quanto à forma do seu cumprimento por empresas que fazem parte do mesmo Grupo.

Mais uma vez orientada pelo princípio da eficiência e sem beliscar os objetivos que se pretendem alcançar, a NOS defende que numa nova versão do Regulamento deverá ficar expressamente prevista a possibilidade de as empresas que constituem uma unidade económica na aceção do artigo 3º da Lei n.º 19/2012, de 8 de maio optarem por dar cumprimento ao Regulamento de forma individual ou de forma integrada, sem prejuízo da assunção da responsabilidade individual de cada uma das empresas.

Tal justifica-se pelo facto de no desenvolvimento da sua atividade normal as referidas empresas poderem ter já, total ou parcialmente, processos partilhados e/ou integrados no que respeita à segurança e integridade das redes e serviços de comunicações eletrónicas. Obrigar a que tais processos sejam autonomizados e replicados em cada uma das empresas que façam parte da mesma unidade económica apenas e só por motivos regulatórios surge como desproporcional e injustificado.

Permitir a opção pelo cumprimento individual ou integrado é a abordagem que melhor acautela a diversidade de situações que podem existir nas empresas em causa, sem prejudicar os objetivos do futuro Regulamento, o que naturalmente é mais eficiente do ponto de vista social. Assim sendo, a NOS solicita que tal possibilidade de opção seja expressamente contemplada no futuro Regulamento.

2.5. Envio de informação à ANACOM

O Projeto de Regulamento, nomeadamente no seu artigo 8º, nº 4, relativo ao inventário de ativos, prevê o envio de informação à ANACOM, incluindo informação sobre a localização geográfica de ativos e identificação das entidades detentoras ou gestoras dos locais.

A NOS tem uma posição muito firme de que não deve ser enviada informação à ANACOM sobre os ativos dos operadores e resultados da análise de risco, bem como outro qualquer envio que descreva a implementação ou funcionamento das arquiteturas, redes e sistemas ou as eventuais vulnerabilidades a que estes possam estar expostos, devido ao risco de fuga de informação, mesmo que inadvertida. [**IIC - Início de Informação Confidencial]** … **[FIC - Fim de Informação Confidencial].** Do ponto de vista da NOS, o preço de uma fuga de informação sobre esta matéria pode ser muito relevante para o país em termos de segurança.

Adicionalmente, não se encontra justificação para o envio de tal informação, uma vez que a mesma estará acessível para consulta diretamente pela ANACOM quando tal for

solicitada e pelos auditores no âmbito das auditorias a realizar, nas instalações dos operadores.

Assim sendo, independentemente da abordagem que a ANACOM venha a adotar quanto ao futuro Regulamento, a NOS entende que o mesmo não deverá prever o envio para a ANACOM, nem para qualquer outra entidade em representação desta, de informação relativa aos seus ativos, incluindo a sua localização geográfica. O envio deste tipo de informação deve ser substituído pela disponibilidade da mesma para consulta pela ANACOM e por outras entidades em sua representação devidamente credenciadas, nas instalações dos operadores e no seguimento de pedido prévio.

2.6. Clarificação das obrigações no âmbito do planeamento de emergência civil, dos planos de emergência e proteção civil e da segurança interna

A NOS considera que é importante que sejam clarificadas as entidades com competência nos diversos domínios da segurança e que as respetivas competências sejam claramente delimitadas, uma vez que atualmente o quadro jurídico – regulamentar não permite concluir de forma inequívoca a cadeia de relações entre as diversas Entidades com competências nesta matéria, nem o modo como elas se interrelacionam. Tal situação cria ineficiências e potencia incumprimentos, inadvertidos, do quadro jurídico – regulamentar e, consequentemente, pode condicionar o atingimento dos objetivos globais fixados no domínio da segurança.

Assim sendo, apela-se à ANACOM que promova, na(s) sede(s) competente(s) a referida clarificação e delimitação e respetiva divulgação pública.

3. Comentários específicos

3.1. Abordagem alternativa: assente no estabelecimento de objetivos de segurança

Na sequência dos comentários gerais, a NOS entende que o Projeto de Regulamento deve ser reformulado no sentido de seguir uma abordagem centrada na fixação de objetivos tendo como referência o documento da ENISA relativo às *Technical Guidelines for Security Measures*.

Note-se que o mapeamento entre os artigos[16] apresentados no Projeto de Regulamento com os domínios e objetivos de segurança (SO) apresentados pela ENISA nas referidas linhas de orientação permite concluir que, conforme se constata na tabela 1, se regista uma correspondência (quase integral)[17] entre os artigos do Projeto de Regulamento e os

[16] Foram considerados os artigos do projeto de regulamento que descrevem obrigações/medidas detalhadas (artigos 7.º a 36.º)
[17] A exceção prende-se com o artigo 11.º, uma vez que a neutralidade de rede não está no âmbito de aplicação dos artigos 13.º e 13.º A da Diretiva Quadro.

SO identificados pela ENISA, inclusive em determinados casos, o mesmo objetivo é acautelado em diferentes artigos do projeto de regulamento.

Assim sendo, conclui-se que as preocupações da ANACOM subjacentes às medidas técnicas de execução e de auditoria incorporadas no Projeto de Regulamento estão acauteladas nos objetivos de segurança estabelecidos nas linhas de orientação da ENISA.

Tabela 1: Mapeamento entre os Artigos do Projeto de Regulamento em consulta e o documento "Technical Guideline on Security Measures" (ENISA, versão 2.0, October 2014)

Artigos	Objetivo de segurança
7	SO 15: Asset management
8	SO 10: Security of supplies SO 15: Asset management
9	SO 2: Governance and risk management
10	SO 10: Security of supplies SO 16: Incident management procedures SO 19: Service continuity strategy and contingency plans SO 20: Disaster recovery capabilities SO 22: Exercise contingency plans SO 23: Network and information systems testing
11	-
12	SO 14: Change management SO 23: Network and information systems testing
13	SO 9: Physical and environmental security SO 11: Access control to network and information systems
14	SO 12: Integrity of network and information systems SO 17: Incident detection capability SO 21: Monitoring and logging policies
15	SO 22: Exercise contingency plans
16	SO 18: Incident reporting and communication
17	SO 1: Information security policy SO 2: Governance and risk management
18	SO 13: Operational procedures SO 16: Incident management procedures
19	SO 18: Incident reporting and communication-
20	SO 3: Security roles and responsibilities
21	SO 3: Security roles and responsibilities
22	SO 3: Security roles and responsibilities
23	SO 25: Compliance monitoring
24	SO 18: Incident reporting and communication
25	SO 18: Incident reporting and communication

26	SO 18: Incident reporting and communication
27	SO 18: Incident reporting and communication
28	SO 25: Compliance monitoring
29	SO 25: Compliance monitoring
30	SO 25: Compliance monitoring
31	SO 25: Compliance monitoring
32	SO 25: Compliance monitoring
33	SO 25: Compliance monitoring
34	SO 25: Compliance monitoring
35	SO 25: Compliance monitoring
36	SO 25: Compliance monitoring

Tendo como base o cruzamento refletido na tabela 1, a NOS apresenta de seguida um exercício ilustrativo da adoção da abordagem preconizada através da alteração de dois artigos do Projeto de Regulamento (artigos 12º e 13º do Projeto de Regulamento) tendo como referência os objetivos de segurança constantes das linhas de orientação da ENISA.

Das linhas de orientação da ENISA é possível extrair os objetivos de controlo a garantir pelos operadores ficando estes com flexibilidade relativamente à escolha dos procedimentos mais ajustados para assegurar o cumprimento dos referidos controlos. Das linhas de orientação é também possível identificar as evidências, isto é, os elementos a serem considerados para demonstração do cumprimento dos controlos predefinidos.

Por exemplo, conforme consta da tabela 1 estão associados ao artigo 12.º do Projeto de Regulamento os SO 14 (Change management) e 23 (Network and information systems testing) do documento da ENISA.

Refira-se que a componente de evidências relativa a cada um dos SO poderá, em termos de redação do futuro de Regulamento, ser agregada num artigo único.

Artigo 12.º Procedimento de Gestão de Alterações

1. As empresas devem estabelecer Procedimentos de Gestão de Alterações a fim de minimizar a probabilidade de ocorrência de incidente de segurança que possa resultar dessas alterações. Para o efeito devem ser:
    a) Seguidos procedimentos operacionais predefinidos previamente à realização de alterações a sistemas críticos *(SO 14)*;
    b) Realizados testes de integração e de sistema previamente à introdução de alterações a sistemas críticos *(SO 23)*.
2. Constitui evidência do cumprimento do estabelecido no número 1:
    a) Documentação com descrição do procedimento operacional para execução de alterações *(SO 14)*;
    b) Relatório da realização dos testes *(SO 23)*.

Artigo 13.º Sistemas de controlo de acessos

1. As empresas devem estabelecer procedimentos de controlo de acessos físicos e lógicos que tenham em especial consideração os ativos constantes do Inventário de Ativos. Para o efeito:
    a. Devem ser implementados procedimentos que detetem ou evitem acessos físicos não autorizados a instalações; *(SO9)*
    b. Devem ser implementados procedimentos de controlo de acesso lógico a ativos que permitam apenas uso autorizado; (*SO11)*
    c. Deve ser avaliada periodicamente a eficácia dos procedimentos de controlo de acesso físico e lógico e realizadas melhorias, se necessário. *(SO9 + SO11)*
2. Constitui evidência do cumprimento do estabelecido no número 1:
    a. Demonstração da implementação de medidas de segurança física; *(SO9)*
    b. Demonstração da implementação de medidas de autenticação e de controlo de acesso dos utilizadores aos ativos; *(SO11)*
    c. Relatório da avaliação da eficácia das medidas de controlo de acesso físico e lógico. *(SO9 + SO11)*

A proposta que acabou de se apresentar deve ser entendida como ilustrativa e visa essencialmente demonstrar o modo como poderá ser feita a evolução do atual Projeto de Regulamento para o ajustar a uma abordagem que respeita a estrutura da Proposta de Regulamento atual mas que se centra no estabelecimento de objetivos de segurança a atingir pelos operadores, a qual, como já amplamente referido apresenta, claros benefícios.

Neste seguimento e de modo a solidificar tal ajustamento, a NOS considera que seria útil a ANACOM promover um grupo de trabalho, envolvendo os operadores, com a missão de contribuir ativamente para a definição concreta do futuro Regulamento.

3.2. Manutenção da abordagem proposta

Sem prejuízo de a NOS entender que a alteração do Projeto de Regulamento focando na definição de objetivos de segurança, admitindo a possibilidade de a ANACOM entender manter a abordagem proposta, apresentam-se de seguida os comentários específicos da NOS às medidas vertidas no Projeto de Regulamento, sendo os mesmos igualmente relevantes na perspetiva de definição do Regulamento numa lógica de objetivos de segurança, conforme proposto pela NOS.

A apresentação destes comentários segue a ordem em que as diferentes matérias surgem na proposta da ANACOM, assumindo particular relevância a necessidade de tornar mais proporcionais e razoáveis as medidas a estabelecer pelo futuro Regulamento, nomeadamente no que respeita à classificação de ativos e inventário, análise de riscos e redundância, resiliência e robustez e respetiva documentação.

3.2.1. Objeto (artigo 1º)

As medidas técnicas e de execução e os requisitos adicionais a cumprir pelas empresas que oferecem redes e serviços de comunicações públicas ou serviços de comunicações eletrónicas devem ser estabelecidas e cumpridas de acordo com o enquadramento comunitário vigente, designadamente o artigo 13-A da Diretiva 2009/140/CE, de 25 de novembro. Ora, este enquadramento está circunscrito à vertente de disponibilidade de serviços e, em conformidade com este enquadramento, a ANACOM tem entendido que o processo de notificação de incidentes de segurança atualmente implementado se restringe a situações que acarretam interrupção de serviços.

A NOS é de opinião que, embora o âmbito do Projeto de Regulamento seja (bem) mais amplo do que o atual mecanismo de notificação de incidentes, a implementação de todas as medidas técnicas e de execução e os requisitos adicionais aí propostos deve-se manter exclusivamente na vertente de interrupção de serviços, em linha com o supramencionado enquadramento dado pelo artigo 13ºA e os serviços relevantes devem continuar a ser os serviços de comunicações percecionados como mais importantes para os cidadãos, entre os quais por exemplo, os serviços de voz e de dados, fixos e móveis e os serviços de televisão paga.

Não devem ser considerados relevantes para efeitos do futuro Regulamento serviços secundários, como são o caso das mensagens multimédia (MMS), serviços de *voice mail,* serviços de subscrição de alertas/músicas/jogos, serviços de portais multimédia, serviços de TV por IP no telemóvel, serviços de dados empresariais desenvolvidos à medida para determinados clientes, entre outros.

3.2.2. Âmbito (artigo 2º)

O Projeto de Regulamento prevê no seu artigo 2º, n.º1 que os operadores devem assegurar o cumprimento das suas obrigações em matéria de segurança e integridade das redes e serviços previstas na lei e no futuro regulamento, em condições normais de funcionamento e em situações extraordinárias, sendo especificado um conjunto de situações consideradas extraordinárias.

Ora, importa alertar que a garantia de cumprimento das obrigações de segurança, designadamente a não interrupção dos serviços, em situações extraordinárias conforme as descritas pode não estar ao alcance dos próprios operadores, na medida em que as redes e ou serviços podem ter sido afetados pelas situações extraordinárias, independentemente das medidas adotadas previamente, e a recuperação das condições de funcionamento poderão não depender dos operadores. Assim sendo, em particular a obrigação prevista na alínea b) do número 1 do artigo 2º, tem que ser considerada de modo relativo.

Neste seguimento é entendimento da NOS que em situações extraordinárias o cumprimento das obrigações previstas deve ser assegurado numa lógica de *best effort* face às condições em cada momento. Aliás, é este o princípio subjacente à obrigação de disponibilidade dos serviços prevista no nº1 do art.º 49 na LCE: *As empresas que oferecem*

serviços telefónicos acessíveis ao público através de redes de comunicações públicas ***devem assegurar a maior disponibilidade possível dos serviços em situações de rutura da rede, situações de emergência ou de força maior****.*

Por sua vez o número 2 do artigo 2º, remete para: i) as obrigações em matéria de disponibilidade dos serviços e de acesso aos serviços de emergência; ii) as obrigações no âmbito do planeamento civil de emergência, dos planos de emergência de proteção civil e da segurança interna; e iii) quando aplicáveis, as obrigações emergentes dos contratos para a prestação do serviço universal.

Ora, no que respeita às obrigações no âmbito do planeamento civil de emergência dos planos de emergência de proteção civil e da segurança interna, reitera-se o exposto nos comentários gerais relativamente à necessidade de clara delimitação e esclarecimento das competências das várias entidades neste domínio. Importa que estejam devidamente definidas as competências de diferentes entidades e organismos que intervêm em temas como o planeamento civil de emergência e planos de emergência de proteção civil e da segurança interna. A clarificação das fronteiras de competências das várias entidades e a sua articulação é essencial para que os operadores conheçam de forma inequívoca e deem cabal cumprimento às suas obrigações nos domínios de segurança, incluindo nas situações de emergência.

O número 2 do artigo 2º refere ainda as obrigações emergentes dos contratos para a prestação do serviço universal. No que respeita à componente de serviços telefónicos do serviço Universal, cuja prestação compete neste momento à NOS, o respetivo contrato estabelece, através da alínea h) da cláusula 7ª (Deveres gerais) que o prestador deve:

(...) Garantir, de forma apta e adequada, o funcionamento dos serviços objeto do presente contrato em situações de crise, emergência ou guerra, incluindo o acesso ininterrupto aos serviços de emergência (...).

Daqui decorre que as obrigações em causa se restringem aos clientes do serviço universal e aos utilizadores que expressamente manifestem interesse em aderir a este serviço em cada momento.

A ANACOM não deve também ignorar que as próprias obrigações que impendem sobre os prestadores do serviço universal de comunicações eletrónicas a partir de um local fixo são suscetíveis de ser impedidas e postas em causa, podendo inclusivamente obrigar à interrupção dos serviços abrangidos, por força de casos de força maior.

Veja-se que a cláusula 20.ª do contrato do serviço universal de comunicações eletrónicas a partir de um local fixo prevê expressamente a suspensão, que pode chegar a ser total, das obrigações emergentes desse contrato quando esteja em causa um evento de força maior, pelo período de duração desse evento.

Nesse âmbito, não há margem para dúvidas que as obrigações do prestador, como deve acontecer no âmbito que aqui nos ocupa, não são de resultado mas de simples meios

Finalmente, o n.º 3 do artigo 2º estabelece que o cumprimento das obrigações deverá ser assegurado para todos os ativos, da propriedade ou da gestão dos operadores, incluindo os equipamentos localizados nas instalações dos clientes.

Ora, o que a ANACOM propõe é em alguns casos inexequível: os operadores nem sempre têm capacidade de intervir e garantir as condições dos equipamentos localizados nas instalações dos clientes, pelo que esta parte da disposição deverá ser eliminada, e em situações em que os ativos não são da propriedade do operador, este muitas vezes não tem capacidade de intervir sobre os mesmos, nomeadamente no âmbito de medidas de segurança como sejam as relativas a redundância, de robustez e de resiliência previstas no artigo 10.º, ou medidas de gestão de alterações previstas no artigo 12º ou sequer garantir aspetos relativos às auditorias.

Assim sendo, as medidas previstas no Projeto de Regulamento deverão ser restritas aos ativos da propriedade do operador ou que estão sobre sua gestão, desde que o operador disponha de total controlo sobre os mesmos. A definição de ativo prevista no artigo 3º deverá ser alinhada com este entendimento.

3.2.3. Definições (artigo 3.º)

No seguimento dos comentários apresentados anteriormente quanto ao perímetro do Projeto do Regulamento, em concreto a sua limitação à vertente de interrupção de serviços, as definições apresentadas no artigo 3º têm que ser sempre e só associadas à continuidade da prestação dos serviços de comunicações eletrónicas.

Esta ressalva é relevante para os conceitos de "ameaça" e "risco", sendo que nestes casos a NOS entende que o âmbito deve estar associado às causas e eventos que resultem numa violação de segurança ou perda de integridade com impacto significativo.

3.2.4. Normalização (artigos 5.º e 30.º)

O Projeto de Regulamento estabelece que as medidas técnicas e organizacionais adotadas para cumprimento das matérias associadas à segurança e integridade das redes devem estar em conformidade com as decisões comunitárias[18] e/ou normas, especificações e recomendações europeias e internacionais, e ainda devem ter em consideração documentos técnicos publicados pela ENISA.

Para este efeito, de acordo com o n.º 3 do artigo 5.º, ANACOM publicará no seu sítio i na internet listagens: (i) das normas, especificações e recomendações europeias e internacionais existentes sobre a matéria; (ii) dos documentos técnicos publicados pela ENISA.

[18] Nomeadamente as adotadas 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 de 2002, relativa a um quadro regulamentar comum para as redes e serviços de comunicações eletrónicas, na sua redação em vigor

A referência ao normativo surge igualmente associada à necessidade de garantir que as auditorias são executadas em conformidade com as normas, especificações ou recomendações europeias e internacionais existentes sobre a matéria, conforme indicado no artigo 30º.

Neste caso, a ANACOM indica, no n.º 2 do artigo 30.º, que este referencial será publicado, também no seu sítio institucional, até ao dia 30 de junho de cada ano.

A NOS entende que o referencial normativo a ser tido em conta pelos operadores no âmbito das suas obrigações de segurança e integridade estabelecidas pelo futuro Regulamento seja submetido a consulta pública e que seja publicado com antecedência adequada face ao prazo limite para os operadores se conformarem ao mesmo, de modo a permitir tempo suficiente de adaptação.

Quanto à periodicidade de publicação das listagens previstas no n.º 3 do artigo 5º nada é referido. Perante esta ausência, a NOS deduz que a mesma corresponda à periodicidade de publicação indicada no n.º 2 do artigo 30.º, *i.e.*, até ao dia 30 de junho de cada ano. o que, a confirmar-se, implicaria a necessidade de adaptação constante dos processos e procedimentos, pelo menos com uma periodicidade anual, algo que se considera pouco razoável. Neste seguimento, a NOS entende e sugere que o referencial normativo observar seja fixado para um período suficientemente alargado, nunca inferior a 5 anos.

3.2.5. Classificação e Inventário de ativos (artigos 7.º e 8.º)

A proposta em consulta prevê que, previamente à realização de um inventário, os operadores procedam a uma classificação dos seus ativos em classes (A a D), em função do impacto de uma interrupção do seu funcionamento.

No que respeita à classificação proposta, a NOS entende os critérios para classificação dos ativos são excessivos e tornam o processo de identificação dos ativos uma tarefa complexa. Assim sendo, sugere-se que estes critérios sejam limitados ao impacto medido em assinantes/acessos (ou área geográfica) impactados por uma interrupção do serviço, mantendo-se a especificidade para Regiões Autónomas, mas sendo eliminados os critérios associados às interligação e centro principal de gestão e operação.

A NOS sugere ainda que a simplificação seja alargada ao número de classes, sendo proposto para o efeito a agregação das quatro classes previstas, em apenas duas classes: ativos críticos e não críticos.

Quanto à classificação dos ativos identificados no âmbito do planeamento civil de emergência ou de um plano de emergência de proteção civil indicado pela ANACOM prevista no nº8 do artigo 7º, a NOS reitera a importância de existir uma plena clarificação sobre quais são as obrigações e âmbito de participação dos operadores no planeamento civil de emergência.

O n.º 2 do artigo 8.º define um conjunto vasto e detalhado de informações a constar sobre cada elemento do Inventário de Ativos, incluindo a localização geográfica e identificação

das entidades detentoras ou gestoras dos locais, o registo de incidentes ocorridos, o registo das alterações efetuadas e a referência à análise de riscos mais recente. Neste sentido, e novamente com o intuito de simplificar o processo e canalizar os esforços para processos mais relevantes, como é o caso da gestão de riscos, a NOS sugere uma reavaliação aos atributos a constar para cada elemento do inventário de ativos.

No que respeita à localização geográfica solicita-se clarificação sobre os dados relevantes a considerar: as coordenadas geográficas ou a morada completa de instalação do ativo.

O registo de incidentes previsto na alínea d) do n.º 2 do artigo 8º deve, no entender da NOS, desde logo por uma questão de proporcionalidade, ser limitado aos incidentes com impacto significativo no funcionamento das redes e serviços e que foram objeto de notificação à ANACOM e/ou informação ao público, nos termos definidos pelo Título III do Projeto de Regulamento.

Relativamente à análise dos riscos mais recente, a NOS sugere a sua eliminação, uma vez que a sua inclusão significaria uma duplicação da documentação prevista no artigo 9º, não sendo por isso justificada ou razoável.

Quanto à inclusão para cada elemento do inventário de ativos do registo das alterações efetuadas, incluindo os resultados dos testes de integração e de sistema realizados e os planos de restauro dos ativos, a NOS sugere que o mesmo seja limitado aos ativos classificados como críticos

Finalmente no que se refere ao envio (comunicação) de informação de inventário para a ANACOM (ou outras entidades) que está previsto no artigo 8º, nº4, remete-se para o exposto nos comentários gerais: a NOS entende que este envio é perigoso devido ao risco de fuga, mesmo que inadvertida, de informação e é desnecessário, uma vez que tais dados estarão sempre disponíveis para consulta pelo regulador ou entidades devidamente credenciadas por este nas instalações dos operadores.

3.2.6. Gestão de riscos (artigo 9.º)

A NOS tem presente a necessidade e importância de uma correta e efetiva análise dos riscos para garantir a segurança e integridade das redes e serviços de comunicações eletrónicas. Este exercício deve, todavia, obedecer a critérios de razoabilidade e eficiência.

Tendo como base este enquadramento, a NOS entende que a proposta de análise de riscos deverá ser simplificada e aliviada em termos de esforço necessário para a concretizar.

Note-se que o Projeto de Regulamento prevê a realização de uma análise de risco global uma vez por ano ou após notificação da ANACOM e a realização de análises de risco parciais que podem ser despoletadas por vários tipos de eventos.

Note-se ainda que, em cada iteração da análise de risco, devem ser considerados vários tipos de ameaças (internas ou externas, intencionais ou não intencionais) e avaliar vários fatores para determinar o impacto e probabilidade de cada risco.

A conjunção da quantidade de análises de risco – globais e parciais - que podem ser executadas durante um ano com o esforço necessário a cada uma delas resulta num esforço total muito elevado para a NOS (e acreditamos que para os restantes operadores). Acresce que a NOS já tem instituídos processos internos de avaliação de riscos que considera adequados e que não são idênticos aos elencados pela ANACOM - apesar de apresentarem inevitáveis pontos de contacto – pelo que se prevê que desta obrigação decorra uma quase duplicação de esforços.

De forma a reduzir o esforço associado a esta obrigação, e no caso de se continuar com uma versão prescritiva da mesma, a NOS considera que as análises de risco globais, despoletadas por uma notificação da ANACOM relativa a um risco, ameaça ou vulnerabilidade, deveriam cingir-se aos ativos que possam ser impactados pelo referido risco, ameaça ou vulnerabilidade e não uma análise de risco global como atualmente proposto no artigo 9º, nº 1, alínea a), ponto ii). A NOS considera que o prazo para realizar uma análise de risco despoletada pela a ANACOM, bem como para a implementação das medidas técnicas e organizacionais que venham a ser definidos em resultado da análise deve ser suficiente. Assim, a NOS defende que o prazo para a realização desta análise não seja inferior a 3 meses após a receção da notificação e adoção de eventuais medidas corretivas não deve ser inferior a 1 ano após a conclusão da referida análise de risco, de forma a contemplar os ciclos de planeamento anuais e *roadmaps* de evolução tecnológica da NOS.

Ainda no âmbito das análises de risco de âmbito global a NOS solicita o esclarecimento sobre quais os ativos que devem ser considerados "*críticos para a continuidade do funcionamento das suas redes ou serviços*"[19], para além dos que serão incluídos nas classes A, B ou C.

Relativamente às análises de risco parciais, estas devem ser realizadas considerando o motivo que as despoletaram. Por exemplo, se uma análise de risco parcial for despoletada pela ocorrência de um incidente com impacto significativo, fará sentido reavaliar o risco do ativo considerando apenas o cenário de falha verificado no incidente.

De forma coerente com os prazos elencados para as análises de risco globais, devem ser previstos pelo menos 3 meses para realização da análise de risco a contar do fim do evento que lhe deu origem e pelo menos 1 ano para adoção de eventuais medidas corretivas.

Relativamente à identificação das ameaças, internas ou externas, intencionais ou não intencionais prevista no nº3 do artigo 9º, tendo presente o esforço e complexidade

[19] Artigo 9º, nº 1, alínea a)

associadas, a NOS entende que este processo deve ser limitado às causas efetivamente relevantes para identificação das ameaças em apreço.

Por último, quanto à possibilidade de a ANACOM emitir, nos termos do n.º8, do artigo 10.º, orientações com vista a uma harmonização da matriz de risco a adotar pelos OPS, a NOS considera trata-se de mais um exemplo de prescrição excessiva por parte da ANACOM que, no âmbito do artigo 9.º. 9.º, não só elenca os critérios a considerar na avaliação de risco como pretende definir o modo de avaliação dos mesmos.

Assumindo que esta precaução é incluída com o objetivo de garantir comparabilidade entre os resultados dos vários operadores, a NOS considera que o resultado relevante do exercício da análise de risco é a identificação de oportunidades de melhoria para a consequente diminuição da probabilidade e/ou impacto de ocorrência de uma interrupção de serviço e não a obtenção e uma classificação para criação de um ranking entre os vários operadores.

3.2.7. Medidas de Redundância, de Robustez e de Resiliência (artigo 10.º)

As medidas de redundância, de robustez e resiliência constituem um bom exemplo da abordagem altamente prescritiva que a ANACOM adotou e que não logrou fundamentar atentos os princípios da adequação e proporcionalidade. Efetivamente a NOS entende que as medidas propostas pela ANACOM nestes domínios para além de serem demasiado detalhadas são excessivas.

Adicionalmente, as propostas apresentadas pela ANACOM suscitam questões de exequibilidade, nomeadamente, a obrigação de assegurar redundância mediante o estabelecimento de ativos alternativos em local geográfico distinto.

No que respeita especificamente às medidas de resiliência em que a ANACOM especifica a duração dos sistemas alternativos de fornecimento de energia em cada uma das categorias de ativos de A a C, é absolutamente necessário uma análise custo-benefício que fundamente tal proposta uma vez que os requisitos são muito exigentes e a sua aplicação integral implicaria um custo muito elevado. Saliente-se a este propósito que os sistemas alternativos de energia são recorrentemente sujeitos a atos de vandalismo ou furtos, pelo que existe não só um custo de implementação inicial como um custo elevado de manutenção e reposição dos mesmos. Pelo exposto, a NOS sugere que esta obrigação seja revista, sendo eliminada a imposição da duração mínima por ativos:

As empresas devem assegurar que os ativos classificados como críticos sejam dotados de sistema de alimentação de energia de emergência que lhes permita ~~assegurar o seu funcionamento~~ minimizar potenciais perturbações ou indisponibilidades ~~em perturbação ou interrupção~~ em caso de interrupção de fornecimento de energia ~~com a seguinte duração mínima:~~

~~a) 24 horas para os ativos classificados na classe A;~~

~~b) 12 horas para os ativos classificados na classe B,~~

~~c) Seis horas para os ativos classificados na classe C.~~

A ANACOM propõe ainda que os testes às medidas redundância, de robustez e de resiliência sejam efetuados com uma periodicidade mínima de 6 meses.

A NOS considera mais uma vez que tal obrigação é excessiva e acarreta riscos, desde logo pelo âmbito alargado dos ativos envolvidos, e porque não se pode afastar a possibilidade de os testes originarem perturbações na prestação dos serviços aos utilizadores finais.

Neste seguimento, a NOS solicita que fique prevista a realização de testes parciais do ponto de vista do número de ativos e o alargamento do prazo previsto no nº.7 do artigo 10.º para a sua concretização.

3.2.8. Procedimentos de controlo da Gestão Excecional de Tráfego no Acesso à Internet (artigo 11.º)

A NOS solicita esclarecimentos quanto ao enquadramento e termos relativos à reserva de capacidade para comunicações de emergência de interesse público, bem como à priorização de tráfego nas situações extraordinárias previstas no atual artigo 11º do Projeto de Regulamento.

Adicionalmente, tendo presente o estipulado no n.º 3 do artigo 3.º do Regulamento (UE) n.º 2015/2120 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015 ("Regulamento TSM"), a NOS têm dúvidas sobre a adequação e grau de detalhe definidos para a recolha da informação, conforme proposto pela ANACOM.

Não obstante as reticências elencadas, a NOS salienta a necessidade de conferir aos OPS flexibilidade para adoção das soluções que considerem adequadas para dar cumprimento à obrigação estabelecida no Regulamento TSM.

3.2.9. Exercícios (artigo 15.º)

A NOS não se opõe à existência de um Programa Anual de Exercícios. Contudo, deverá ficar prevista a possibilidade de os exercícios serem realizados de forma faseada para os ativos constantes do Inventário, *i.e.*, em cada exercício poderá estar envolvido um número limitado de ativos e não a totalidade do portfólio constante do referido inventário. Salienta-se que esta abordagem foi a seguida pelo regulador belga (IBPT), estabelecendo a realização de testes limitados aos ativos críticos e a inclusão de todos os ativos classificados como críticos nos testes num espaço de 3 anos[20].

Quanto à proposta de envolvimento de outros operadores ou de terceiras entidades na execução do Programa Anual de Exercícios, a NOS entende que esta participação deverá ser assegurada numa lógica de *best effort* e sugere-se que a ANACOM assuma o papel de

[20] Fonte: Cullen International. Não foi imposta pelo regulador belga uma classificação de ativos organizada em classes, sendo conferida ao OPS a possibilidade de priorizar os ativos em função da sua importância

dinamizador e coordenador dos exercícios conjuntos (intra e extra setor das comunicações eletrónicas).

3.2.10. Prestação de informação aos clientes (artigo 16.º)

A NOS considera que a comunicação com os seus clientes é feita por canais próprios e nos termos adequados aos destinatários em função dos seus interesses, podendo tal estar vertido e especificado em termos contratuais.

A NOS não antecipa qualquer vantagem de impor aos operadores de comunicações a obrigação de prestarem informações sobre segurança a um conjunto especifico de clientes. Com efeito, não se percebe de que modo a imposição de tal comunicação irá contribuir para melhorar a segurança e integridade das redes e serviços de comunicações eletrónicas.

Se tal comunicação for considerada relevante e valorizada pelo cliente, a existência e moldes da comunicação que melhor respondem às necessidades do cliente em causa serão previstas do ponto de vista contratual.

De notar que a NOS efetua, de forma transparente para o cliente, intervenções frequentes sobre a rede e sistemas que suportam a prestação de serviços ao cliente, de forma a garantir cada vez melhores níveis de serviço, pelo que os clientes seriam alvo de um número elevado de comunicações, provocando dúvidas e entropia desnecessária.

Quanto ao envio em simultâneo desta comunicação à ANACOM, recorda-se que o regulador terá conhecimento das medidas adotadas na sequência do envio da notificação final, nos termos dos n.º 8 e 9 do artigo 25.º do projeto de regulamento, pelo que a NOS considera que a obrigação prevista no artigo 16º é redundante e deverá ser também eliminada.

Acresce que a NOS tem dúvidas quanto à fundamentação para que a ANACOM seja informada sobre as ações de melhoria implementadas com impacto num único cliente, quando não está em causa a prestação de serviços de comunicações eletrónicas a utilizadores finais.[21]

Por fim, de acordo com *benchmark* efetuado, salienta-se que nenhum regulador europeu, nem mesmo a PTS, impõe requisitos de comunicação para um conjunto específico de clientes.

[21] Veja-se por exemplo o alargamento de conceito de cliente relevante a setores, por exemplo, como o transporte e a energia,

3.2.11. Responsável de Segurança (artigos 2.º, 6.º, 8.º, 17.º, 20.º, 23.º, 25.º, 34.º a 36.º, 37.º)

Atendendo às responsabilidades atribuídas ao Responsável de Segurança, é expectável que a função venha a ser atribuída a um colaborador com elevada posição hierárquica na empresa.

Sucede que para além dos deveres previstos no artigo 20º relativos à política de segurança e sistema de gestão de segurança, está também associada a esta função um conjunto de tarefas repetitivas e frequentes, incluindo a assinatura da notificação final prevista nos termos dos n.º 8 e 9 do artigo 25.º do Projeto de Regulamento.

Ora, não parece razoável exigir que o Responsável de Segurança tenha que garantir de forma exaustiva esse conjunto de tarefas. Assim, em complemento à designação de um Responsável de Segurança, a NOS sugere que seja conferida a possibilidade da designação, voluntária e opcional, de um Responsável de Segurança adjunto que pode assumir as funções do Responsável de Segurança na ausência deste ou de constrangimento de outra ordem que limitem a respetiva disponibilidade.

Face ao exposto, a NOS sugere o ajustamento aos artigos aplicáveis[22], de forma a prever a possibilidade de designação de um Responsável de Segurança adjunto que partilha as funções acometidas ao Responsável de Segurança.

3.2.12. Ponto de contacto permanente e ponto de contacto alternativo (artigos 17.º, 21.º)

A designação do ponto de contacto alternativo deve ser efetuada pelos operadores que detenham ativos classificados nas classes A ou B, sendo que a mesma deve ser assegurada, nos termos do n.º 3 do artigo 21.º, em local geograficamente distinto do local onde é assegurada a função de Ponto de Contacto Permanente.

A NOS sugere que, em alternativa ao local geograficamente distinto, a função de ponto de contacto alternativo possa ser acessível através de uma rede de comunicações alternativa à do OPS (e do Ponto de Contacto Permanente).

3.2.13. Equipa de resposta a incidentes de segurança (artigo 22.º)

Em linha com os comentários previamente apresentados, a NOS entende que o âmbito de intervenção da Equipa de Resposta a Incidentes de Segurança prevista no artigo 22.º está limitada aos incidentes de segurança que impliquem interrupção dos serviços relevantes.

[22] Artigos 2º, 6º, 8º, 17º, 20º, 23º, 25º, 34º a 36º, 37º

3.2.14. Dossier de Segurança (artigo 23.º)

No artigo 23º está prevista a obrigação de compilar e manter atualizado um dossier de segurança, o qual deverá conter versões históricas dos últimos 5 anos. A NOS questiona a adequação e proporcionalidade da manutenção deste registo histórico, quando muito admite-se que possa existir um registo de alterações face à versão anterior.

Adicionalmente, a NOS entende como excessiva a obrigação prevista de manter as cópias de todas as notificações e divulgações realizadas ao abrigo do disposto no Título III, respeitantes aos incidentes de segurança ocorridos nos últimos cinco anos, sobretudo quando a ANACOM já dispõe do registo destas mesmas notificações. Ainda que seja justificável a manutenção de um registo dos incidentes notificados, a NOS sugere a eliminação da obrigação de preservar no Dossier de Segurança, as cópias das notificações efetuadas.

Por último, a propósito do dossier de segurança deverá ser clarificado que a manutenção do dossier poderá ser feita em suporte eletrónico e não físico e que assinatura prevista no nº 5 poderá ser eletrónica/digital.

3.2.15. Obrigações de notificação (artigos 24º e 25º)

A ANACOM optou por transpor para o Projeto de Regulamento a deliberação de 12 dezembro de 2013 relativa às circunstâncias, formato e procedimentos aplicáveis às exigências de comunicação de violações de segurança ou perdas de integridade com impacto significativo no funcionamento das redes de comunicações públicas e dos serviços de comunicações eletrónicas acessíveis ao público, incluindo alguns ajustamentos.

Entre os referidos ajustamentos está a inclusão de dois novos clientes relevantes (RNSI – Rede Nacional de Segurança Interna e SRPCBA – Serviço Regional de Proteção Civil e Bombeiros dos Açores) e a futura inclusão, a partir da data de notificação pela ANACOM, dos operadores de serviços essenciais a identificar no âmbito da aplicação do diploma de transposição da Diretiva (UE) n.º 2016/1148 e dos proprietários ou operadores de infraestruturas críticas designadas ao abrigo do disposto no Decreto-Lei n.º 62/2011.

Conforme previsto no artigo 25º da Diretiva (UE) n.º 2016/1148, a transposição para legislação nacional deverá ocorrer em 2018, sendo que a designação das entidades, nos termos do anexo II inclui os seguintes setores (e subsetores): energia, transportes, banca, infraestruturas do mercado financeiro, setor da saúde, fornecimento e distribuição de água potável e infraestruturas digitais.

Quanto aos proprietários ou operadores de infraestruturas críticas, o Decreto-Lei n.º 62/2011 prevê a inclusão dos seguintes setores: energia e transportes.

Assim, através desta "mera" disposição a ANACOM propõe atribuir a designação de clientes relevantes a um vasto conjunto de intervenientes em diferentes setores e

respetivos subsetores [23], resultando desta forma num tratamento diferenciado em matérias de segurança e com um ónus adicional para os operadores.

A NOS entende que o alargamento do número de clientes relevantes deverá ser efetuado de forma faseada, privilegiando os setores mais relevantes e para os quais as comunicações eletrónicas são efetivamente determinantes na prestação dos serviços aos seus utilizadores.

Adicionalmente, o tratamento privilegiado que, na prática resulta da classificação de cliente relevante, apenas deveria ter que ser prestado a partir do momento que for recíproco. Esta situação é particularmente relevante se tivermos em conta que estamos perante setores dos quais existe uma elevada dependência do setor das comunicações eletrónicas, com destaque para as empresas do setor energético.

Neste contexto, a NOS entende que cabe à ANACOM um papel determinante na promoção junto do regulador setorial da energia (ERSE) para garantir que os operadores de comunicações eletrónicas são incluídos no conceito de clientes prioritários nos termos do artigo 63.º do Regulamento n.º455/2013 (Regulamento de Qualidade de Serviço do Setor Elétrico). Tal permitiria garantir um tratamento mais equitativo entre os *players* dos dois setores e proporcionaria um tratamento mais célere dos incidentes que afetam a disponibilidade de serviços de comunicações eletrónicas, mitigando desta forma os impactos para os utilizadores finais.

Ainda no que respeita ao setor energético, tendo presente as competências conferidas à ANACOM na alínea b) do art.º 2.ºA da LCE, a NOS apela a que o regulador setorial sensibilize as autoridades competentes para a necessidade de garantir aos operadores de comunicações um acesso prioritário a meios/recursos eventualmente necessários em situação de emergência/catástrofe (e.g., combustíveis para alimentação dos sistemas de energia socorrida) com o objetivo de garantir maior celeridade na reposição dos serviços prestados.

Adicionalmente, em cenários de emergência/catástrofes, e sempre que não seja possível garantir remotamente a reposição dos serviços, devem ser assegurados aos operadores meios de acesso às suas instalações/infraestruturas, ainda que as mesmas estejam em locais interditos e/ou de difícil acesso.

Quanto aos patamares associados às obrigações de notificação das violações de segurança ou das perdas de integridade com impacto significativo no funcionamento das redes e serviços, a ANACOM não efetuou nenhuma alteração à deliberação de 12 de dezembro de 2013. A este respeito, a NOS reitera o seu entendimento de que o patamar cumulativo de ≥8 horas de impacto/ 5.000> n.º de assinantes ou de acessos afetados ≥

[23] Refira-se a existência de setores que se encontram abrangidos por ambos os documentos legais, nomeadamente a energia e os transportes

1.000 deve ser revisto ou, em alternativa, ajustado, prevendo o envio mensal de relatórios que agregassem estas ocorrências.

O Projeto de Regulamento mantém a obrigação de envio da notificação final, através de entrega em mão ou de correio registado, sendo que a mesma deverá ser assinada pelo Responsável de Segurança. Com vista à minimização do esforço administrativo e de custos associados ao envio através de entrega em mão ou de correio registado, a NOS reforça a sugestão para que também as notificações finais possam ser enviadas para um endereço de correio eletrónico, formato que acarreta ainda a vantagem de permitir a receção imediata por parte da ANACOM, sendo que já atualmente existem múltiplas comunicações de e para a ANACOM que são transmitidas através desta via. Adicionalmente, este formato de transmissão permite acautelar a obrigatoriedade da assinatura pelo Responsável de Segurança, neste caso por meio de uma assinatura digital certificada.

3.2.16. Auditorias à segurança das redes e serviços (artigos 28.º a 36.º)

A NOS reconhece que algumas preocupações elencadas na sua resposta ao "Início de procedimento de elaboração de um Regulamento relativo à segurança e integridade das redes e serviços" foram acautelados na proposta de Regulamento, nomeadamente no que respeita ao planeamento e calendarização.

Genericamente, a NOS concorda com os prazos propostos pela ANACOM para as diferentes fases do processo, salvo num ponto em específico: envio do Relatório da Auditoria, que nos termos previstos pelo n.º 4 do artigo 35º implica o envio deste documento, assinado em nome da Auditora e, com conhecimento do Responsável pela Segurança, no prazo de 10 dias úteis a contar da conclusão das atividades da Fase de Auditoria.

Atendendo a que, em muitos, casos, são necessárias iterações adicionais entre a empresa auditora e as entidades auditadas até que seja acordado um relatório final, a NOS sugere que o prazo de 10 dias úteis para envio do Relatório de Auditoria seja contabilizado a partir da aceitação pela entidade auditada do Relatório e não a partir da conclusão das atividades da Fase de Auditoria, como agora está previsto, de modo a acautelar situações imprevistas e que exijam interações adicionais.

Em linha com os comentários ao objeto e âmbito do Projeto de Regulamento, as auditorias devem ser efetuadas com vista a aferir o cumprimento de medidas de segurança associadas à interrupção dos serviços.

Neste sentido, as medidas que venham a ser apresentadas no Plano de Correção das Não Conformidades devem ser limitadas à vertente de continuidade de prestação do serviço. Para além disso, devem ser ponderadas e avaliadas tendo em máxima consideração o racional económico para a imposição de cada medida, atendendo aos custos de implementação e manutenção *vis-à-vis* o retorno económico associado, assim como os planos de evolução tecnológica implementados pelos operadores, de forma a evitar a

realização de investimentos em tecnologias, arquiteturas ou serviços que serão alterados ou descontinuados a curto/médio prazo.

Quanto ao dever de colaboração previsto no artigo 32.º, sem prejuízo do compromisso de colaboração e assistência necessárias para a realização das Auditorias nos termos previstos, a NOS entende que todo e qualquer contacto que venha a ser realizado com os fornecedores relevantes ao nível da segurança e integridade das redes e serviços deverá ser feito por intermédio do próprio operador e deverá acontecer apenas e só quando existam sérias e fundamentadas dúvidas sobre os resultados da auditoria. ~

Finalmente, a NOS entende que deve ser avaliada a possibilidade da realização das auditorias em modelo *self-assessment* e/ou pelas equipas de Auditoria Interna dos operadores. Estes modelos de permitem atingir os propósitos previstos e, simultaneamente, minimizar os custos associados. Mais, estes modelos têm a vantagem de serem conduzidos por elementos com conhecimento dos sistemas, processos e procedimentos implementados pelos operadores, o que apresenta uma grande mais-valia no resultado final.

4. Conclusão

A NOS partilha dos objetivos subjacentes aos Projeto de Regulamento em consulta e reconhece mérito à proposta apresentada pela ANACOM.

No entanto, a NOS considera que a ANACOM não logrou fundamentar as propostas concretas apresentadas designadamente à luz do regime definido por outros reguladores comunitários de referência, como são o caso da OFCOM e da COMREG, bem assim do risco do país, em geral, e das medidas implementadas pelos operadores nacionais e respetivo risco, em particular. Acresce que a ANACOM, ao contrário do que se considera ser adequado, não apresentou qualquer análise custo-benefício que justifique o nível de exigência refletido no Projeto de Regulamento.

Na verdade, atendendo ao enquadramento nacional e comunitário, a NOS entende que as medidas propostas pela ANACOM são excessivas e demasiado prescritivas.

A NOS sugere a adoção de uma abordagem alternativa, que à semelhança de reguladores de referência já mencionados, assenta no estabelecimento de objetivos de segurança descritos pela ENISA nas suas *Technical Guideline for Security Measures*. Esta abordagem acautela as preocupações subjacentes às propostas da ANACOM ao mesmo tempo que permite maior flexibilidade aos operadores quanto às medidas concretas a adotar para atingir os objetivos, o que permite maior eficiência na afetação de recursos.

Em qualquer caso, a NOS entende como necessária a reformulação do Projeto de Regulamento de modo a garantir a proporcionalidade e razoabilidade das medidas a definir pela ANACOM. Neste sentido, a NOS propõe, entre outros, a revisão dos requisitos relativos ao inventário de ativos e sua classificação, à análise de riscos, das medidas de redundância, resiliência e robustez,

Neste seguimento, a NOS sugere que a ANACOM promova um grupo de trabalho com os operadores com vista a reformular o Projeto de Regulamento no sentido de o tornar mais razoável e proporcional atenta a realidade nacional e o enquadramento nacional e comunitário que o enforma.