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

Comentários da NOS

03 de outubro de 2018

Sumário Executivo **3**
1. Introdução **5**
2. Comentários específicos **5**
2.1. Objeto (art.º 1º) 5
2.2. Âmbito (art.º 2º) 6
2.3. Meios eletrónicos (art.º 5º) 8
2.4. Normas (art.º 6º e 27º) 8
2.5. Medidas técnicas de segurança (art.º 7º) 9
2.6. Classificação de ativos (art.º 8º) 11
2.7. Inventário de ativos (art.º 9º) 13
2.8. Requisitos da gestão dos riscos (art.º 10º) 14
2.9. Procedimentos de Controlo da Gestão Excecional (art.º 11º) 14
2.10. Exercícios (art.º 12º) 16
2.11. Informação aos clientes relevantes (art.º 13º) 16
2.12. Ponto de contacto permanente e Equipa de resposta a incidentes (art.º 15º e 16º) 17
2.13. Plano de segurança (art.º 17º) 18
2.14. Relatório anual de segurança (art.º 19º) 18
2.15. Obrigações de notificação à ANACOM (art.º 21º e 22º) 19
2.16. Obrigações de informação ao público (art.º 23º e 24º) 20
2.17. Auditorias (art.º 25º e 33º) 21
3. Conclusão **22**

Sumário Executivo

A NOS congratula a ANACOM pela opção em submeter a consulta pública uma segunda versão do projeto de regulamento de segurança, sobretudo quando foram acolhidas algumas propostas apresentadas no âmbito do primeiro procedimento de consulta concluído no 1º trimestre de 2017.

Concretamente, a NOS saúda a alteração à abordagem na imposição das medidas técnicas de execução e de requisitos adicionais, com o cumprimento de requisitos prescritivos a ser substituído pela adoção de objetivos de segurança, conforme proposta apresentada pela generalidade dos operadores presentes no mercado. Adicionalmente, a NOS destaca como positivas as simplificações introduzidas nos requisitos exigidos à fase de auditoria, assim como a indicação imediata das normas que devem servir de base às medidas técnicas e procedimentos de auditoria.

Contudo, foram mantidas determinadas obrigações que mereceram fundamentadas reservas por parte da NOS na sua resposta ao primeiro projeto de regulamento, pelo que pelo que estes aspetos são reiterados nos comentários específicos.

Desde logo, não obstante o esforço da ANACOM em incorporar nesta versão uma abordagem mais flexível, assente na prossecução de objetivos de segurança, a NOS considera que o regulador poderia ter ido ainda mais longe nesta flexibilização, sendo de notar que, em alguns casos, preocupações associadas às 11 medidas especificas adicionais estão acauteladas pelos objetivos de segurança. Efetivamente existem redundâncias entre medidas previstas pelos objetivos de segurança e as medidas específicas adicionais, conforme demonstram os requisitos da gestão dos riscos (art.º 10º) e plano de segurança (art.º 17º).

A NOS entende ainda que a obrigação em assegurar o cumprimento dos níveis de sofisticação 1 e 2 para todos os objetivos de segurança deve prever um atingimento faseado, de forma a permitir maior viabilidade e adequação das medidas de segurança adotadas.

Quanto à classificação de ativos, a NOS mantém a divergência de fundo quanto à classificação em classes nos termos propostos pela ANACOM.

Sem prejuízo, a ser mantida esta abordagem, no caso dos ativos a serem incluídos na classe A, a NOS entende que o regulador deve rever a opção de inclusão nesta classe de todos os ativos dos clientes relevantes, assim como clarificar especificidades dos ativos associados à prestação de serviços nas Regiões Autónomas (RA).

Em relação ao inventário de ativos, merecem especiais reservas a decisão da ANACOM em manter a inclusão das coordenadas geográficas e identificação das entidades detentoras dos ativos, assim como devem ser indicadas quais as funcionalidades e serviços a serem considerados. Adicionalmente, deve ser eliminada a referência a que o impacto deve incluir termos de redundância, robustez e resiliência.

No que se refere aos clientes relevantes, a NOS defende a eliminação do tratamento preferencial previsto para comunicação em caso de ocorrências que afetem a prestação de serviços de comunicações eletrónicas a estes clientes, assim como a ANACOM deve avaliar a forma como pretende concretizar o alargamento do número de clientes relevantes.

No que diz respeito à compilação documental prevista para o Plano de segurança e Relatório anual, a NOS entende que os requisitos associados devem ser aligeirados, de forma a garantir que o esforço burocrático é ajustado e proporcional, face aos objetivos associados. Com efeito, o Plano de segurança deverá estar limitado à Política de segurança, sendo que no Relatório anual devem ser eliminados os requisitos associados à descrição das atividades desenvolvidas, recolha estatística sobre incidentes com e sem impacto, análise agregada de ocorrências e indicação do programa de exercícios do ano seguinte ao relatório.

A respeito dos procedimentos para gestão de tráfego, a NOS questiona a alteração do prazo de implementação proposto de 18 meses para 80 dias, sendo este prazo incomportável com as exigências necessárias à concretização desta obrigação. Adicionalmente, NOS defende que o regulamento a aprovar deverá prever uma consulta ao mercado para uma caracterização de alto nível dos conceitos envolvidos neste artigo, sendo que o prazo de implementação do disposto neste artigo, apenas deverá iniciar-se após conclusão desse procedimento.

Relativamente às obrigações de notificação à ANACOM, a indicação das freguesias e respetivos concelhos afetados pela violação de segurança deverá ser limitada à notificação final, uma vez que somente nesta fase é possível dar com maior precisão o impacto geográfico do incidente.

Acerca das obrigações de notificação ao público, a NOS questiona o retrocesso verificado com a forte redução do prazo máximo de publicação nos websites das ocorrências com impacto significativo de 4 horas úteis para 1 hora corrida, sendo que a ANACOM deve apresentar uma justificação plausível para esta alteração, que acarreta impactos que foram previamente reconhecidos no passado.

Para a NOS não devem existir dúvidas que o âmbito de aplicação do futuro regulamento deve ser circunscrito à vertente de disponibilidade dos serviços, e mais especificamente a situações que acarretam interrupção na prestação dos serviços de comunicações eletrónicos percecionados como mais importantes para os utilizadores.

Ainda no que respeita ao âmbito de aplicação, a NOS defende que as medidas previstas no futuro 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 NOS defende que cada operador deve ter a possibilidade de decidir a forma como concretiza a equipa de resposta a incidentes, sem que tal implique obrigatoriamente a constituição de uma equipa formal ou com elementos fixos.

Finalmente, a NOS apresenta propostas de simplificação dos requisitos a serem cumpridos na escolha das auditoras, dado que as propostas da ANACOM limitam de forma excessiva a disponibilidade de empresas que possam cumprir com as condições impostas.

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 segundo projeto de regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas ("segundo projeto de regulamento").

Nos comentários específicos, expostos por artigo, a NOS reitera alguns pedidos de esclarecimentos apresentados na sua resposta à primeira consulta, e que não mereceram resposta por parte da ANACOM.

Adicionalmente, são apresentadas propostas fundamentadas de revisão medidas tendo em especial atenção a manutenção de obrigações e/ou introdução de novos requisitos, sem que estes sejam justificados ou impliquem, no entendimento da NOS, o aumento da segurança e resiliência das redes e serviços de comunicações eletrónicas, objetivo primordial que deve pautar a proposta de regulamento.

2. Comentários específicos

2.1. Objeto (art.° 1°)

No âmbito das competências específicas atribuídas à ANACOM, e que justificaram a elaboração do presente projeto de regulamento, está a fixação de medidas adequadas para garantir a integridade das redes com vista a assegurar a continuidade da prestação dos serviços que se suportam nas referidas redes.

Estas competências surgem enquadradas pelos artigos 54.°-A, n.° 1 do artigo 54.°-C e no artigo 54.°-D da Lei das Comunicações Eletrónicas (LCE)[1].

Neste contexto, destaca-se o previsto no n.° 2 do artigo 54.°A, segundo o qual as empresas que prestam serviços de comunicações eletrónicas devem adotar as medidas adequadas para garantir a integridade das respetivas redes com o intuito de assegurar a continuidade da prestação dos serviços que se suportam nestas redes.

Face a este enquadramento, para a NOS não existem dúvidas que o âmbito de aplicação das medidas técnicas e de execução, requisitos adicionais e processo de notificação de incidentes, que sejam fixadas no futuro regulamento, deve ser circunscrito à vertente de disponibilidade dos serviços de comunicações eletrónicas, e mais especificamente a situações que acarretam interrupção na prestação destes serviços.

De igual modo, para a NOS é também inequívoco que a esfera de intervenção do futuro Regulamento deve ser limitada aos 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. Aliás, não se encontram quaisquer justificações ou racional para que sejam impostas obrigações aos serviços de comunicações eletrónicas secundários, como por exemplo as mensagens multimédia (MMS) ou serviços de *voice mail,* bem como outros serviços de comunicações eletrónicas

[1] Lei n° 5/2004, na sua redação atual

que não façam parte do âmbito das obrigações de reporte de informação estatística à ANACOM.

Assim sendo, a NOS não compreende o esclarecimento prestado pela ANACOM no relatório da consulta pública sobre o projeto de regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas de julho de 2018 de que não pode "*limitar, em geral e a priori, o âmbito de aplicação deste projeto*".[2]

Em resumo, a NOS defende que a ANACOM deve indicar claramente no regulamento final que o objeto das obrigações previstas está circunscrito à vertente de continuidade da prestação dos serviços de comunicações eletrónicas, devendo estes serviços serem claramente identificados nos termos supra apresentados.

Como último ponto, a NOS reitera a necessidade de a ANACOM prever explicitamente a possibilidade de cumprimento conjunto do regulamento por empresas do mesmo grupo.

Para o efeito, no futuro regulamento deve ser 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.

Este procedimento garante a eficiência na aplicação de recursos por parte dos operadores, nomeadamente quando já detêm processos integrados ou partilhados, garantindo também por este meio maior nível de segurança e resiliência.

2.2. Âmbito (art.º 2º)

De acordo com o previsto neste artigo, os operadores devem garantir que o cumprimento das suas obrigações em matéria de segurança e integridade das redes e serviços ocorre em condições normais de funcionamento e em situações extraordinárias devidamente elencadas.

A NOS não pode deixar de reiterar os comentários previamente apresentados de que em determinadas situações extraordinárias pode não estar ao alcance dos operadores o cumprimento das obrigações de segurança, designadamente a continuidade na prestação dos serviços, na medida em que as redes e ou serviços podem ter sido afetados, independentemente das medidas adotadas previamente. O mesmo se aplica à recuperação das condições de funcionamento, que poderá também não depender exclusivamente dos operadores.

Por isto, não deixa de ser iníquo exigir aos operadores de comunicações eletrónicas o mesmo grau de cumprimento das obrigações de segurança e integridade das redes e serviços nas situações previstas nos números 2 e 3 do artigo 2º. Na verdade, nos cenários descritos, a NOS considera que salvo organismos ou entidades públicas com intervenção direta na gestão de acidentes graves ou catástrofes, nenhuma outra empresa pública ou privada tem a capacidade de assegurar o mesmo nível de segurança que os garantidos em condições normais de funcionamento.

[2] p. 11

Face ao exposto, a NOS reforça a necessidade de revisão desta obrigação no sentido de que, em situações extraordinárias, o cumprimento das medidas de segurança previstas no futuro regulamento deverá ser efetuado numa lógica de *best effort*.

Quanto às obrigações previstas no n.º4 do artigo 2º, contrariamente ao indicado pela ANACOM no Relatório da consulta pública sobre o projeto de regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas de julho de 2018[3], continuam a não ser claras as fronteiras de competências das várias entidades em matérias de planeamento civil de emergência dos planos de emergência de proteção civil e da segurança interna. Assim, reitera-se o pedido para que a ANACOM, como regulador setorial, proceda a uma devida clarificação do papel das empresas e entidades competentes, de forma a garantir que todos conhecem de forma inequívoca o seu papel e possam dar cumprimento às suas obrigações nos domínios de segurança, incluindo nas situações de emergência.

A NOS questiona ainda a manutenção da alínea c) do referido n.º 4 do artigo 2º, uma vez que, conforme demonstrado na resposta ao primeiro projeto de regulamento, as obrigações emergentes dos contratos para a componente de serviços telefónicos do serviço universal são restritas aos clientes do serviço universal e aos utilizadores que expressamente manifestem interesse em aderir a este serviço em cada momento.

Neste sentido, a referência constante da suprarreferida alínea c) deve refletir esta restrição, devendo ser ajustada de forma a indicar que se tratam das obrigações emergentes dos contratos para a prestação do serviço universal, aplicáveis aos assinantes desta oferta.

Por fim, reiteram-se os comentários anteriormente apresentados quanto à inexequibilidade de os operadores serem obrigados a assegurar o cumprimento das obrigações de segurança para os ativos que não da sua propriedade ou gestão, incluindo os equipamentos localizados nas instalações dos clientes.

No caso específico dos equipamentos localizados nas instalações dos clientes existem constrangimentos que limitam a capacidade de intervenção das empresas sujeitas às obrigações de segurança, nomeadamente nos casos em que:

i. a propriedade do equipamento é do operador, mas a sua gestão é da responsabilidade dos clientes (algo que acontece com maior frequência nos clientes particulares)
ii. a propriedade do equipamento é do cliente, mas a sua gestão é da responsabilidade dos operadores (cenário comum a clientes empresariais)

Por isto, dado que os operadores nem sempre têm capacidade de intervir e garantir as condições dos equipamentos localizados nas instalações dos clientes, as obrigações em matéria de segurança e integridade das redes e serviços, previstas na lei e no projeto de regulamento, devem ser explicitamente limitadas aos ativos da propriedade do operador ou que estão sobre sua gestão, desde que o operador disponha de total controlo sobre os mesmos.

[3] p.11

2.3. Meios eletrónicos (art.° 5°)

De acordo com o indicado neste artigo, a ANACOM prevê o desenvolvimento de um sistema de informação que permita a partilha por parte dos operadores dos elementos demonstrativos do cumprimento das obrigações impostas de notificação, comunicação, acesso e cooperação.

A NOS reitera as suas preocupações quanto aos riscos inerentes à disponibilização a terceiros de elementos sensíveis, classificados como confidenciais. Estes receios são fundamentados pelo facto de que, inegavelmente, a partilha de informação potencia vulnerabilidades de segurança. Com efeito, uma potencial fuga de informação, mesmo que inadvertida, de elementos como os incluídos no Relatório Anual de Segurança pode acarretar sérios prejuízos para os operadores e mesmo para a segurança nacional.

Sem prejuízo desta discordância de princípio por parte da NOS, caso a ANACOM mantenha as obrigações de partilha de informação sensível, os meios eletrónicos que venham a ser usados devem comprovadamente dispor de certificação e serem dotados de robustas medidas de segurança na transmissão, acesso e armazenamento da informação disponibilizada.

Consequentemente, caso os meios eletrónicos de partilha não estejam concluídos à data de entrada em vigor do primeiro envio de dados à ANACOM, este envio não poderá ser efetuado por correio eletrónico. Nesta eventualidade, a partilha de informação deverá ser substituída pela consulta de informação sensível por parte de elementos da ANACOM, devidamente credenciados e habilitados, diretamente nas instalações dos operadores.

2.4. Normas (art.° 6° e 27°)

A NOS entende que as normas elencadas na alínea b) do n°2 do artigo 6°, que devem servir de base às medidas técnicas e organizacionais e os requisitos adicionais adotados pelos operadores para cumprimento do disposto na lei e no presente regulamento, constituem uma referência adequada.

Contudo, salientamos que conforme decorre da redação da referida alínea, na ausência de decisões previstas na alínea a) do n°2 do artigo 6°, estas normas devem servir como base ou referência, não decorrendo daqui qualquer obrigação de que as medidas implementadas sejam integral e globalmente assentes nestas normas.

Neste sentido, a NOS propõe um texto alternativo em que seja indicado que "*as empresas devem adotar um conjunto de medidas técnicas e organizacionais que sejam baseadas ou compatíveis com uma seleção de normas (...)*", entre as quais se encontram as normas exemplificadas na alínea b) do n°2 do artigo 6°.

No que respeita à obrigação vertida no artigo 27°, a NOS salienta que o cumprimento das normas indicadas está impreterivelmente dependente da existência no mercado de empresas auditoras independentes que assegurem o seu cumprimento, pelo que a obrigação este artigo deverá ser revista de forma a ser acautelada esta condicionante.

Para o efeito a NOS propõe um texto alternativo em que seja indicado que "*As empresas devem assegurar que as auditorias são realizadas com recurso a um conjunto de requisitos que sejam baseados ou compatíveis com as normas* (....).

2.5. Medidas técnicas de segurança (art.° 7°)

A NOS reconhece o esforço desenvolvido pela ANACOM em incorporar no presente projeto de Regulamento de Segurança a proposta apresentada pelos operadores e APRITEL em substituir algumas medidas prescritivas por uma abordagem mais flexível, assente na prossecução de objetivos de segurança.

Em contrapartida, a NOS considera que a imposição da obrigação de assegurar os níveis de sofisticação 1 e 2 para todos os objetivos de segurança é desproporcionada.

Pese embora a existência de um período de 18 meses, após aprovação da versão final do regulamento, para adoção das medidas e a possibilidade de derrogação prevista na alínea a) do n°1 do artigo 7°, a NOS entende que no futuro Regulamento deve ser previsto um atingimento faseado destes níveis de sofisticação.

Para este propósito, a NOS apresenta a seguinte proposta:

i. Atingimento do **nível 1** de sofisticação (básico) para **80%** do âmbito dos 25 objetivos de segurança no prazo de **18 meses** após entrada em vigor do regulamento ou início de atividade do operador

ii. Atingimento do **nível 2** de sofisticação (norma da indústria) para **80%** do âmbito dos 25 objetivos de segurança no prazo de **36 meses** após entrada em vigor do regulamento ou início de atividade do operador

Com efeito, a proposta de definição de um patamar de 80% do âmbito de cumprimento justifica-se pela constatação de que em determinados objetivos de segurança o operador poderá apresentar já o atingimento de medidas de níveis superiores, sem necessariamente estar a cumprir todas as medidas de segurança dos níveis de sofisticação precedentes.

Para melhor ilustrar este facto vejam-se os seguintes exemplos:

i. **"Objetivo de segurança 9 (Segurança física e ambiental)**: podem estar já implementadas pelo operador as medidas de segurança previstas para o nível de sofisticação 3, por exemplo "*avaliar periodicamente a eficácia dos controlos físicos e ambientais*", sem que necessariamente estejam aplicadas medidas previstas para o nível 1, como "*manter procedimentos de proteção*" para cenários catastróficos tais como "tornados" ou "sismos ou maremotos. Este caso acontece, por exemplo, nas medidas adotadas para riscos de catástrofe, dado que o investimento em medidas específicas de proteção acarreta um custo que poderá ser incomportável para alguns operadores;

ii. **Objetivo de segurança 22** (**Exercícios de planos de contingência**): novamente, podemos estar perante um cenário em que uma medida de nível 3 como "*envolver nos exercícios fornecedores e outros terceiros, nomeadamente outras empresas, parceiros de negócio*" esteja implementada, mas que outra de nível 2 como "*a utilização de cenários variáveis ao longo do tempo*", não esteja efetivada.

Neste contexto, a proposta da NOS permite adequar os objetivos de segurança aos procedimentos já implementados pelos operadores, sem que seja exigido o esforço de implementação de medidas de proteção onerosas e injustificadas.

Para além do cumprimento dos objetivos de segurança, o nº 3 do artigo 7º prevê ainda que os operadores implementem 11 medidas específicas adicionais.

Ora, tal como demonstrado na tabela infra, as preocupações subjacentes a algumas destas 11 medidas especificas estão acauteladas pelos 25 objetivos de segurança e correspondentes medidas de segurança. Aliás, em alguns casos, existe mesmo uma correspondência efetiva entre as medidas específicas adicionais e os objetivos de segurança.

Sendo essencial garantir que as obrigações impostas não resultam num esforço desproporcional para os operadores, nos comentários a cada um dos correspondentes artigos que as enquadram, a NOS propõe rever ou mesmo eliminar medidas específicas redundantes.

Tabela 1: Comparação entre objetivos de segurança e medidas específicas

Art.º	**Medidas específicas**	**Objetivos/medidas de segurança** que correspondem às medidas especificas:	**Avaliação da NOS**
8º	Classificação de ativos	**15:** Gestão dos ativos **14:** Gestão de alterações	Manter com ajustes
9º	Inventário de ativos		Manter com ajustes
10º	Requisitos da gestão dos riscos	**2:** Governação e gestão dos riscos	Eliminar
11º	Procedimentos de Controlo da Gestão Excecional de Tráfego de Acesso à Internet	**21:** Políticas de monitorização e registo de eventos [parcialmente]	Manter com ajustes
12º	Exercícios	**22**: Exercícios de planos de contingência	Manter com ajustes
13º	Informação aos clientes	**18:** Notificação e comunicação de incidentes de segurança	Manter com ajustes
14º	Responsável de segurança	**3**: Funções e responsabilidades no domínio da segurança [parcial] **3:** Funções e responsabilidades no domínio da segurança [parcial]	Manter
15º	Ponto de contacto permanente		Manter com ajustes
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]	Manter com ajustes
17º	Plano de segurança	**1:** Política de segurança **3:** Funções e responsabilidades no domínio da segurança **16**: Procedimentos de gestão de incidentes de segurança	Eliminar, mantendo apenas a Política de Segurança
18º	Deveres específicos de comunicação à ANACOM	**3**: Funções e responsabilidades no domínio da segurança [parcial]	Manter
19º	Relatório Anual de Segurança	**16:** Procedimentos de gestão de incidentes de segurança [parcial] **22:** Exercícios de planos de contingência [parcial]	Manter com ajustes

2.6. Classificação de ativos (art.º 8º)

A NOS mantém a divergência de fundo quanto à classificação em classes nos termos propostos pela ANACOM.

Com efeito, a NOS reitera o entendimento de que a alternativa mais razoável compreende uma classificação binária, entre ativos críticos e não críticos, em termos a serem alinhados entre o regulador e operadores.

Acresce que, conforme demonstrado na tabela 1, os objetivos de segurança 14 e 15 cobrem globalmente o exigido pelos artigos 8º e 9º, uma vez que para efetuar a "gestão dos ativos e de controlo de configurações", bem como a "gestão de alterações", operador tem de identificar, classificar e elaborar um cadastro dos seus ativos. Assim sendo, a NOS defende que cada operador deve ter a possibilidade de proceder à classificação dos seus ativos em função dos critérios de risco identificados.

Apesar da proposta de simplificação de classes avançada pela ANACOM, subsiste o entendimento da NOS de que a atual proposta mantém um elevado e injustificado grau de exigência e complexidade.

Aliás, este é reforçado porque neste segundo projeto de regulamento a ANACOM optou, sem que tenha apresentado razões que justifiquem a abordagem, por agregar na classe A[4] as anteriores classes A e B do primeiro projeto em consulta, aplicando a ambos os critérios de classificação dos ativos da classe A, que são mais exigentes.

Acerca dos ativos de classe A, estes continuam a abranger os "*ativos de que dependa a oferta de redes e serviços através dos quais seja assegurada a continuidade da prestação dos serviços previstos na alínea f) do n.º 2 do artigo 21.º*".

Assim, nos termos da alínea c) do n.º 3 do artigo 8º, devem ser incluídos todos os ativos de que dependam:

i. os clientes relevantes já identificados - SIRESP, RNSI, SRPCBA
ii. os operadores de serviços essenciais,
iii. os operadores de infraestruturas críticas,
iv. outras entidades que a ANACOM pode livremente designar no prazo de 5 dias úteis.

A NOS entende que a ANACOM deverá reavaliar a obrigação de inclusão de todos os ativos dos clientes relevantes e/ou que venham a ser designados pela ANACOM.

No caso dos clientes relevantes já identificados, pela sua natureza de atuação em situações de emergência ou crise, entidades do tipo SIRESP e RNSI devem possuir as suas próprias capacidades de resiliência para assegurar a continuidade da prestação dos serviços. Portanto, a NOS defende que este ónus não deve ser também imposto aos operadores de comunicações eletrónicas, sobretudo quando estes não têm relação direta no âmbito de atuação destas entidades.

[4] Sobre a qual recaem as obrigações de segurança mais exigentes

Quanto aos operadores de serviços essenciais[5] e operadores de infraestruturas críticas[6] tratam-se na maioria dos casos de empresas com redes de distribuição e presença nacional capilares. Desta forma, num contexto em que a ANACOM propõe que as obrigações de segurança abranjam todos os ativos que suportam os clientes relevantes, incluindo os equipamentos localizados nas instalações dos clientes relevantes sob gestão do operador de comunicações eletrónicas, estaríamos perante um cenário em que um número injustificado de ativos das redes fixas e móveis poderiam ser incluídos na classe A.

A NOS entende que tal desvirtua por completo a segmentação de criticidade que se pretende com a existência de 3 classes de ativos, assim como agrava a complexidade associada à gestão de informação e caracterização propostas neste projeto de regulamento para os ativos de classe A.

Por último, a inclusão imediata de todos os ativos na classe A não deve envolver quaisquer entidades designadas pela ANACOM, pelo menos no prazo de 5 dias úteis associado a esta designação, dado que o mesmo não permite as necessárias adaptações que possam resultar de uma alteração entre classes de ativos.

Face ao exposto, a NOS propõe que o âmbito dos ativos associados aos clientes relevantes deve:

i. ser acordado entre o operador de comunicações eletrónicas e o respetivo cliente relevante, devendo o âmbito do acordo estar centrado nos serviços críticos que servem o cliente relevante
ii. alternativamente, no caso de não existir acordo entre as partes, seguir os critérios previstos no nº 2 e nas alíneas a), b) e d) do nº3.

Na identificação e classificação dos ativos, merece ainda comentários da NOS o previsto na alínea e) do nº 3, artigo 8º, segundo o qual devem ser classificados na classe A "*os ativos que tenham sido identificados no âmbito do planeamento civil de emergência ou de um plano de emergência de proteção civil e que a ANACOM indique através de comunicação com a identificação do ativo*".

A este propósito, a NOS relembra que os operadores disponibilizaram uma relação das suas infraestruturas críticas físicas à Autoridade Nacional da Proteção Civil e, anteriormente, ao Conselho Nacional Planeamento Civil de Emergência (CNPCE / CPEC).[7]

Em consequência, a NOS entende que os ativos abrangidos por esta obrigação devem corresponder aos que foram indicados no âmbito desta identificação de infraestruturas críticas. Neste contexto, a ANACOM, no âmbito das suas atribuições e competências, nomeadamente em matéria de planeamento civil de emergência e de proteção civil, pode ter acesso aos elementos partilhados com as suprarreferidas entidades, sem que exista a necessidade e riscos de uma nova partilha de informação.

Ainda no que respeita aos ativos a serem classificados na classe A, de acordo com o nº 2 do artigo 8º, devem ser incluídos os ativos que em resultado de perturbação no seu funcionamento seja afetada a prestação de serviços na totalidade do território de uma ilha

[5] Cuja futura designação envolverá empresas de setores como a distribuição de energia, transportes, prestadores de cuidados de saúde, instituições bancárias, prestadores de infraestruturas digitais

[6] Presentes em setores como a energia e transportes

[7] Informação disponibilizada em 2016 à ANPC e anos anteriores ao extinto CNPCE

da RA dos Açores ou da RA da Madeira, assim como devem ser, tal como descrito na alínea d) do nº3, considerados nesta classe os ativos que assegurem a interligação inter e intra ilhas das RA.

A este respeito não é claro para a NOS o que deve ser considerado como a "totalidade" do território de uma ilha. Por exemplo, num cenário em que o operador forneça apenas serviço a parte de uma das ilhas das RA, não é claro se os ativos devem ser imediatamente considerados na classe A ou se a sua classificação deverá ser ponderada em função dos outros critérios enunciados.

Em resumo, a NOS defende que a ANACOM deve reavaliar a inclusão de todos os ativos dos clientes relevantes na classe A, assim como deve clarificar o entendimento que deve ser considerado com a afetação na prestação dos serviços na totalidade do território de uma ilha da RA dos Açores ou da RA da Madeira.

2.7. Inventário de ativos (art.º 9º)

A ANACOM mantém a obrigação de elaborar e manter um inventário de ativos, tendo como base a classificação prevista no art.º 8 e um conjunto alargado de detalhes adicionais.

Na perspetiva da NOS, o detalhe solicitado é excessivo e oneroso, o que resulta numa enorme complexidade na manutenção da informação e caraterização exigida para os ativos das classes A e B, quer do ponto de vista administrativo, quer do ponto de vista de modelo de identificação de todos os elementos exigidos.

Efetivamente, a NOS considera que o esforço burocrático é imposto sem que seja claro de que forma uma inventariação prescritiva contribui para que os operadores alcancem um maior nível de segurança nas suas redes.

Deste modo, a NOS propõe que a listagem apresentada no nº 2 do artigo 9º seja entendida como uma orientação que os operadores devem ter em linha de conta na elaboração e manutenção do seu inventário de ativos, a ser estruturado com os dados que estes considerem como mais relevantes para atingirem os objetivos de segurança.

A ANACOM manteve ainda neste projeto de regulamento a partilha anual de elementos sensíveis, obrigação objeto de reservas fundamentadas por parte da NOS, conforme comentários ao artigo 5º. Reitera-se a este propósito a posição da NOS de que esta obrigação deve ser substituída pela consulta de informação sensível por parte de elementos da ANACOM, devidamente credenciados e habilitados, diretamente nas instalações dos operadores.

Os riscos associados a esta partilha de informação são ainda maiores se considerarmos que nesta relação estão incluídos elementos como as coordenadas geográficas da sua localização e a identificação das entidades detentoras ou gestoras dos locais.

No que respeita à caracterização prevista na alínea a) do n.º 3, a NOS considera que a ANACOM deve desde já explicitar quais as funcionalidades e serviços que devem ser considerados, que devem corresponder aos serviços de comunicações eletrónicas referidos nos comentários ao artigo 1º, ou seja, os serviços de voz e de dados, fixos e móveis e os serviços de televisão paga.

Por fim, a NOS entende que a referência à fundamentação da classificação do ativo prevista na subalínea ii) da alínea a) do nº 3 deverá ser limitada ao impacto potencial de

uma perturbação do seu funcionamento, conforme decorre dos critérios de classificação de ativos proposto no n.º2 do artigo 8º. Nesta perspetiva deverá ser eliminada a referência a que o impacto deve incluir "*termos de redundância, robustez e resiliência*".

2.8. Requisitos da gestão dos riscos (art.º 10º)

A NOS não compreende a necessidade de imposição desta medida específica quando existe um objetivo de segurança – objetivo 2: Governação e gestão dos riscos – que permite acautelar que os operadores têm esse processo de segurança implementado de forma adequada.

Ademais, a NOS não reconhece qualquer vantagem em impor aos operadores a revisão da metodologia pelo menos uma vez em cada dois anos, sobretudo quando a metodologia de gestão de riscos é um elemento basilar, sendo recomendado que a mesma se mantenha estável ao longo do tempo de maneira a ser eficaz na identificação dos riscos e na avaliação dos ativos.

Na verdade, o que faz sentido é determinar uma revisão periódica aos ativos, utilizando para o efeito uma metodologia de gestão dos riscos, algo que já está previsto pelas medidas de segurança incluídas no objetivo 2.

Neste sentido, a NOS propõe a eliminação desta medida.

2.9. Procedimentos de Controlo da Gestão Excecional (art.º 11º)

O presente artigo não apresenta alterações substanciais ao conteúdo plasmado no anterior projeto de decisão, com a exceção da remoção do n.º 4 com a qual a NOS concorda.

Assim sendo, a NOS mantém as mesmas reservas apresentadas na anterior consulta relativamente à adequação do detalhe de informação apresentado no n.º 2, tanto mais que não é evidente quais as medidas técnicas concretas de gestão de tráfego que se enquadram no âmbito do presente artigo.

Com efeito, o presente regulamento não densifica o conceito de gestão temporária ou excecional de tráfego, relativamente ao regulamento 2015/2120 do Parlamento de Europeu e do Conselho.

Ora, esta incerteza dificulta não só o entendimento sobre as práticas de gestão de tráfego em apreço, como a avaliação do impacto da preparação dos sistemas dos prestadores para recolher o detalhe solicitado, que se afigura excessivo.

A título de exemplo, atente-se ao disposto na alínea a) do número 2 deste artigo:

"... A exceção que a fundamenta, nos termos previstos nas alíneas a), b) ou c) do 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, devidamente documentada; ..."

Quando é referido que as exceções deverão ser devidamente documentadas, os requisitos específicos da caracterização (e comprovação) da exceção constituem um elemento essencial para a implementação da obrigação imposta. Não se pretende com isto uma definição determinística e fechada da parte do regulador destes requisitos, até porque

serão os operadores que melhor poderão determinar quais os elementos que melhor responderão ao objetivo pretendido.

Mas para que essa definição possa ser feita pelos operadores, é necessário que orientação adicional seja dada ao mercado, de modo a permitir aos operadores identificar a informação que melhor responderá a esse objetivo. Caso contrário, corre-se o risco de cada operador ter uma interpretação distinta da dos demais e, nenhuma delas, corresponder ao objetivo pretendido pelo regulador, o que implicará custos adicionais para o setor e litigância indesejável.

Neste contexto, o regulamento a aprovar deverá prever uma consulta ao mercado para uma caracterização de alto nível dos conceitos envolvidos neste artigo, sendo que o prazo de implementação do disposto neste artigo, apenas deverá iniciar-se após conclusão desse procedimento.

No que respeita ao prazo para a sua implementação, e independentemente do universo e definições em causa, a NOS considera particularmente preocupante a redução substancial do prazo de entrada em vigor.

Relembra-se que, no anterior projeto de decisão, estava previsto que os procedimentos de controlo de gestão excecional de tráfego de acesso à Internet entrassem em vigor no prazo de 18 meses. Porém, o projeto atualmente em consulta reduz, inexplicavelmente e sem enquadramento, este prazo para 80 dias.

O anterior prazo afigurava-se indispensável para (1) o alinhamento de entendimento, entre todos os *stakeholders*, sobre as definições e critérios para a classificação de práticas de gestão de tráfego temporárias e extraordinários, bem como para (2) a implementação nos sistemas dos instrumentos necessários para dar resposta às exigências de informação incluídas no n.º 2 do artigo em apreço.

A este respeito, cumpre lembrar que a implementação técnica das medidas preconizadas requer, necessariamente, um processo interno de levantamento de requisitos e de validação da sua compatibilidade com as ferramentas existentes, seguido de um processo de *procurement* que passa pela auscultação junto dos fornecedores das soluções disponíveis no mercado, do lançamento de concurso para a contratação da solução, da negociação do contrato com o fornecedor selecionado e, só então, da implementação e teste da solução final. Ora, tendo presente o atrás exposto, nomeadamente da necessidade de densificação dos conceitos associados à obrigação que impende sobre os operadores, um prazo de 80 dias úteis é manifestamente insuficiente e inviabiliza o cumprimento das obrigações pelos operadores.

Assim, a NOS exorta ao regulador e revisão do prazo previsto no presente projeto, revertendo para o prazo previsto no anterior projeto.

Adicionalmente, também para esta medida especifica, o objetivo de segurança 21 - Políticas de monitorização e registo de eventos já prevê de medidas destinadas a "manter sistemas e funções de monitorização e de registo de eventos relativos aos ativos classificados" que permitem acautelar as preocupações elencadas, incluindo os requisitos exigidos no nº 3 do artigo 11º para "monitorização do tráfego de acesso à Internet, de modo contínuo, para a deteção: a) de riscos à segurança e integridade da rede, dos serviços prestados através dela e dos equipamentos terminais dos utilizadores finais; b) de congestionamentos iminentes da rede".

2.10. Exercícios (art.º 12º)

A NOS acolhe positivamente a decisão da ANACOM de alargar a periodicidade do programa de exercícios para bianual.

Ainda que o objetivo de segurança 22 (Exercícios de planos de contingência) preveja a realização de exercício de planos de contingência e de redundância, sempre que necessário em colaboração com terceiros, a NOS não se opõe à manutenção desta medida específica, desde que os requisitos prescritos sejam revistos.

Desde logo, ainda que a periodicidade tenha sido alargada, a NOS entende que a mesma não deve ser vinculativa, assim como o âmbito dos ativos sujeitos aos exercícios deve ser definido por cada operador em função dos riscos identificados.

Mais, a NOS entende não existirem quaisquer razões que justifiquem a imposição de tratamento preferencial para os ativos de clientes relevantes em matéria de exercícios, pelo que esta disposição deve ser eliminada da versão final do Regulamento.

2.11. Informação aos clientes relevantes (art.º 13º)

No relatório da consulta pública sobre o projeto de regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas de julho de 2018, a ANACOM justifica o reforço das disposições relativas à proteção dos clientes relevantes com a "*criticidade dos serviços prestados pelos clientes em causa e, por outro, ao aumento da dependência da prestação desses serviços em relação às redes e serviços de comunicações eletrónicas em que se suportam*".[8]

Ocorre que este ónus adicional para os operadores acontece sem que no sentido inverso os operadores possam beneficiar de qualquer tratamento preferencial. Com efeito, se por um lado é real a crescente importância dos serviços de comunicações eletrónicas para a sociedade em geral, por outro lado, entre os clientes relevantes estão incluídos setores dos quais existe uma elevada dependência do setor das comunicações eletrónicas, com destaque para as empresas do setor energético.

Acresce que a ANACOM prevê, através da alínea d) do n.º5 do artigo 21º, o alargamento do conceito de clientes relevantes aos operadores de serviços essenciais e aos proprietários ou operadores de infraestruturas críticas.

Portanto, assiste-se à possibilidade de alargamento das obrigações previstas para esta categoria de clientes a um vasto conjunto de *stakeholders*, presentes em setores tão distintos como o financeiro, saúde ou abastecimento de águas, que passam a ter desta forma num tratamento diferenciado quanto à forma de comunicação de ocorrências na prestação dos serviços de comunicações eletrónicas contratados.

Note-se ainda que estas obrigações são impostas quando existe grupos de trabalho, nomeadamente promovidos pela ANPC, em que são discutidas medidas de proteção e resiliência entre operadores e clientes relevantes.

Dado que a NOS presta, de forma voluntária e transparente, as devidas informações aos clientes, em canais próprios e nos moldes adequados às suas necessidades, reiteramos o

[8] p.26

entendimento de que não se antecipam quaisquer vantagens na imposição de obrigações de prestação de informações sobre segurança a um conjunto especifico de clientes.

A mesma oposição é válida para a obrigação de os operadores comunicarem a estes clientes, com conhecimento da ANACOM, as medidas adotadas na sequência de incidentes de segurança que tiveram impacto na continuidade dos serviços de comunicações eletrónicas contratados. A partilha desta informação com os clientes relevantes coloca em causa a confidencialidade da informação sobre incidentes e sobre as medidas de segurança dos operadores de comunicações eletrónicas. Os clientes, por mais relevantes que sejam, não devem por defeito ser destinatários deste tipo de informação.

Aliás, a NOS não compreende, nem a ANACOM justifica, qual o racional para ser informada, antecipadamente à receção da notificação final prevista nos n.º 8 e 9 do artigo 22º, sobre as medidas de segurança implementadas com impacto num conjunto específicos de entidades, que não são prestadores de serviços de comunicações eletrónicas a utilizadores finais.[9]

Pelo exposto, demonstrada a desadequação das medidas propostas, a NOS solicita que as obrigações de informação associadas aos clientes relevantes sejam suprimidas da versão final do Regulamento.

2.12. Ponto de contacto permanente e Equipa de resposta a incidentes (art.º 15º e 16º)

A NOS compreende o racional implícito à imposição de um ponto de contato permanente, com a capacidade de iniciar e de receber um fluxo de informação de nível operacional e técnico entre a empresa e a ANACOM.

Contudo, as referências à ativação e a operacionalização dos procedimentos fixados no âmbito do planeamento civil de emergência ou de plano de emergência da proteção civil constantes nas alíneas c) e d) do nº 1 do artigo 15º suscitam dúvidas quanto ao papel a ser desempenhado por este ponto de contacto permanente e pela ANACOM.

A este respeito, a NOS reitera os comentários apresentados no artigo 2º quanto à necessidade de uma inequívoca clarificação quanto às competências das várias entidades em matérias de planeamento civil de emergência dos planos de emergência de proteção civil e da segurança interna.

No que respeita à equipa de resposta a incidentes, a NOS entende que sem prejuízo do estrito cumprimento das obrigações previstas, cada operador deve ter a possibilidade de decidir a forma como concretiza esta equipa, sem que tal implique obrigatoriamente a constituição de uma equipa formal ou com elementos fixos, conforme decorre da definição de colaboradores-chave apresentada na alínea f) nº1 do artigo 3º.

Esta flexibilidade permite uma adaptação dos meios alocados à resolução das violações de segurança ou perda de integridade que, pela sua variabilidade quanto às causas e impacto, pode exigir elementos com competências específicas.

Neste sentido, os elementos da equipa de resposta a incidentes de segurança não devem ser abrangidos pela lista de colaboradores-chave a ser incluída na alínea d) do nº1 do artigo

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

17º, nem serem objeto do procedimento descrito no nº3 do artigo 17º de demonstração dos comprovativos de se encontram devidamente mandatado, nos termos legalmente previstos, para representar a empresa no exercício da função.

Salienta-se que, conforme demonstrado na tabela 1, o objetivo de segurança 3 (Funções e responsabilidades no domínio de segurança) já preveem uma estrutura adequada de funções e responsabilidades no domínio da segurança das redes e serviços, pese embora não explicitar as figuras do Responsável de segurança ou Ponto de contacto permanente.

Finalmente, refira-se que a NOS possui pontos de contacto permanente, comunicados periodicamente à ANPC, sendo que estes pontos possuem os meios de contacto alternativos e principais referidos no nº 4 do art.º 15º.

2.13. Plano de segurança (art.º 17º)

A NOS concorda com a proposta de elaboração e manutenção de uma Política de Segurança, tal como previsto no nº1, alínea a), por entender que a mesma é adequada e condizente com os princípios subjacentes à elaboração de um plano de segurança.

Aliás, salientamos que a existência de uma política de segurança é um dos objetivos de segurança a que se a que se refere a alínea a) do artigo 7.º (objetivo 1).

Em contrapartida, a NOS questiona a inclusão dos requisitos previstos nas alíneas b) (descrição de todas as medidas), c) (registo de incidentes com maior impacto nos últimos 5 anos) e d) (lista de colaboradores chave) no Plano de segurança, uma vez que entendemos que as preocupações implícitas a estes requisitos se encontram 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).

Ademais, para as três alíneas, estamos perante requisitos onerosos, excessivos e associados a uma elevada carga burocrática documental, não sendo claro de que forma a sua inclusão contribui para a concretização de um Plano de Segurança que permita aos operadores atingirem um maior nível de segurança das redes.

Um exemplo que ilustra esta constatação prende-se com a imposição de incluir comprovativos de que cada colaborador chave se encontra devidamente mandatado para representar a empresa no exercício da função que lhe foi cometida, obrigação sobre a qual a NOS não vislumbra valor acrescentado para o cumprimento de requisitos de segurança.

Face ao exposto, a NOS considera que a obrigação de disponibilização de um Plano de Segurança deverá ser revista de forma a incluir apenas a Política de Segurança desenvolvida por cada operador.

2.14. Relatório anual de segurança (art.º 19º)

Na proposta de regulamento em consulta, o Relatório anual de segurança surge como a principal compilação documental, função que havia sido acometida na primeira proposta de regulamento ao Dossier de segurança, obrigação no entanto eliminada desta nova versão.

Neste contexto, foram introduzidos um conjunto de requisitos adicionais ao Relatório anual de segurança, conferindo a esta obrigação uma carga burocrática e documental que

a NOS entende como excessiva, sem que para tal sejam enunciadas as correspondentes vantagens na sua concretização.

Consequentemente, a NOS defende a necessidade de aligeirar ou mesmo eliminar alguns dos requisitos propostos para o Relatório anual de segurança.

O primeiro prende-se com a descrição das atividades desenvolvidas em matéria de segurança das redes e serviços indicada na alínea a) do n. º1, que a NOS considera que deve ser limitada aos ativos classificados como críticos. Este entendimento justifica-se pelo facto de que, como a ANACOM terá certamente presente, são diariamente empreendidas inúmeras ações com vista a garantir a segurança das redes e serviços dos operadores. Assim sendo, a inclusão neste relatório anual de todas as atividades desenvolvidas representa uma excessiva e injustificada carga burocrática e documental.

Em segundo lugar, a NOS defende a eliminação da recolha estatística prevista na alínea b) do n.º 1, dado que com a notificação dos incidentes de segurança que cumpram com os patamares indicados no artigo 21º, a ANACOM dispõe dos elementos para a elaboração de estatísticas sobre o número de ocorrências com impacto significativo.

No caso dos incidentes sem impacto significativo, a NOS relembra que estas ocorrências não são relevantes face às regras e patamares definidos no projeto de regulamento. Acresce que, a ser entendida de forma literal, implicaria o registo e compilação de todas as ocorrências que resultem na interrupção de serviços, mesmo que estas sejam limitadas a um único cliente e a um período residual.

Quanto ao previsto na alínea c) do n.º 1, o envio dos elementos solicitados ao abrigo da notificação de incidentes de segurança e perdas de integridade fornece à ANACOM os indicadores necessários à realização de uma análise agregada dos incidentes com maior impacto, com a mais-valia de que o regulador dispõe dos dados de todos os operadores presentes no mercado. Portanto, não se antecipando vantagens para que este ónus seja transmitido aos operadores, a NOS considera que esta análise deve ser suprimida.

Relativamente à descrição, prevista na alínea d) do n.º 1, do programa de exercícios que abranja o ano civil seguinte ao qual o relatório anual de segurança se reporta, a NOS entende que a mesma deve ser opcional, mantendo-se apenas a obrigatoriedade de indicação do programa de exercícios do ano a que respeita o relatório. Com efeito, pode não ser exequível, com a antecedência pretendida, proceder a uma identificação precisa dos ativos e/ou serviços que serão sujeitos à realização de exercícios.

Finalmente, caso à data de entrada em vigor do primeiro envio do Relatório não estejam implementados os meios eletrónicos de partilha de informação previstos no artigo 5º, a NOS solicita esclarecimentos quanto à necessidade de manutenção de suporte físico dos documentos incluídos no Relatório anual de segurança.

Em suma, a NOS defende que os requisitos relativos ao registo de todas as atividades desenvolvidas em matéria de segurança, a recolha estatística de incidentes com e sem impacto, tal como o programa de exercícios do ano seguinte ao relatório devem ser eliminados do Relatório anual de segurança.

2.15. Obrigações de notificação à ANACOM (art.º 21º e 22º)

No n.º 7 do artigo 22º que estabelece os parâmetros a serem considerados na notificação de fim de violação de segurança ou perda de integridade com impacto significativo, foram

introduzidas novas exigências, incluindo a indicação das "freguesias e respetivos concelhos" afetados pela violação de segurança.

A NOS identifica de imediato constrangimentos em assegurar de forma precisa esta informação, sobretudo no prazo de duas horas após o fim da ocorrência. Na verdade, 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 NOS entende que indicação concreta das zonas afetadas deverá ser limitada à notificação final.

Em linha com os esclarecimentos solicitados sobre a classificação de ativos associados às RA, para efeitos de cumprimento da alínea e) do nº2 do artigo 21º, solicita-se clarificação quanto ao entendimento sobre o impacto o funcionamento de todas as redes e serviços oferecidos por uma empresa na totalidade do território de uma ilha. Em concreto deve ser clarificada a forma como devem ser considerados os casos em que a prestação de serviços por um dado operador esteja limitada apenas a determinadas zonas geográficas.

Novamente, a NOS alerta para os impactos associados ao alargamento do número de clientes a serem incluídos na categoria clientes relevantes, previsto na alínea d) no n.º 5 do artigo 21º. Assim, de acordo com o previsto na alínea f) do nº2 do artigo 21º, teriam que ser notificados à ANACOM todos os incidentes com duração superior a 30 minutos desde que tenha impacto num qualquer cliente relevante, o que é manifestamente desproporcionado.

A ser mantido, a NOS entende que o alargamento deve 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.

2.16. Obrigações de informação ao público (art.º 23º e 24º)

Através da alínea ii) do n.º 1 do artigo 24.º é introduzida a obrigação de publicação das zonas impactadas por uma ocorrência com desagregação ao nível da freguesia.

Ora, dado que determinadas ocorrências, nomeadamente as calamidades naturais (incêndios, intempéries, outros) podem afetar zonas geográficas alargadas abrangendo um vasto número de freguesias, incluindo todas as freguesias de um dado concelho, a NOS defende que esta obrigação deve ser descrita de forma a prever explicitamente flexibilidade no seu cumprimento, de forma a não comprometer a transparência e clareza nas informações prestadas aos utilizadores.

Contrariando a indicação que a execução das obrigações de notificação e de divulgação ao público tem vindo a decorrer de uma forma eficaz e consensual, a ANACOM vem propor uma alteração significativa ao processo de divulgação de público, sem que para o efeito apresente qualquer justificação para esta decisão.

Esta alteração implica a redução do atual prazo de disponibilização da informação no site das atuais 4 horas úteis (decorridas entre as nove e as dezanove horas de um dia útil) para 1 hora após a notificação inicial.

Acontece que este prazo de 1 hora foi descartado pela ANACOM na sequência dos comentários apresentados pelos operadores ao sentido provável de decisão de 22 de

Dezembro de 2011[10]. Aliás, salienta-se que no correspondente relatório da consulta pública a ANACOM justificou a sua decisão por terem sido ponderados os argumentos expostos como a distribuição horária ao longo das 24 horas, quer quanto ao custo do trabalho quer quanto à relevância da divulgação da informação.[11] Esclarece-se e alerta-se para o facto da comunicação efetuada em *website,* destinada ao publico e aos clientes, ser diferente da notificação à ANACOM e utilizar uma linguagem própria, adequada ao contexto e de acordo com a política de comunicação do operador de comunicações. A comunicação ao público e a clientes é elaborada e aprovada por equipas diferentes da equipa técnica que assegura as notificações à ANACOM.

Dado que os comentários apresentados na referida consulta[12] se mantêm válidos, a NOS considera que esta proposta de alteração do prazo deve ser excluída, devendo ser mantido o atual prazo de notificação ao público no prazo de 4 horas úteis (decorridas entre as nove e as dezanove horas de um dia útil) após a notificação final de uma ocorrência.

2.17. Auditorias (art.° 25° e 33°)

Relativamente aos requisitos que devem ser acautelados na realização de auditorias, a NOS salienta que o cumprimento de exigências com a prevista na alínea b) do n° 1 do artigo 28° está condicionado pela existência no mercado de empresas auditoras com o nível de experiência indicado.

Acresce que para além os requisitos indicados no n°1 do artigo 28°, a escolha das auditoras está também condicionada pela necessidade de assegurar as condicionantes previstas nos números 2 e 3, associadas a potenciais conflitos de interesses e rotatividade na escolha das auditoras.

A NOS entende que os critérios são excessivos e desproporcionais, podendo mesmo tornar inexequível a escolha de uma empresa auditora, dada a possibilidade de não existirem empresas no mercado que cumpram com todos os requisitos definidos.

Assim, de forma a minimizar os riscos de não serem encontradas empresas que cumpram com os critérios fixados, sugere-se a eliminação do n.° 3, uma vez que a generalidade das auditoras procede à rotatividade dos colaboradores envolvidos em processos de auditorias recorrentes.

Adicionalmente, qualquer colaborador da ANACOM que tenha intervenção nos processos de auditoria deverá estar sujeito, por uma questão de equidade, aos critérios que venham a ser estipulados para as auditoras e seus colaboradores, incluindo credenciação adequada emitida por entidades competentes para acesso a matéria classificada e entrega de declarações de inexistência de conflitos de interesses.

---

[10] Sobre as circunstâncias, formato e procedimentos aplicáveis à comunicação das violações de segurança ou das perdas de integridade com impacte significativo no funcionamento das redes e ou serviços de comunicações eletrónicas acessíveis ao público

[11] Relatório da Audiência prévia e do procedimento geral de consulta lançado a 22 de dezembro de 2011, p. 61

[12] E que resultou na deliberação de 12 de dezembro de 2013, relativa às circunstâncias, ao formato e aos procedimentos aplicáveis às exigências de comunicação de violações de segurança ou perdas de integridade com impacte significativo no funcionamento das redes de comunicações públicas e dos serviços de comunicações eletrónicas acessíveis ao público, bem como à divulgação ao público, por parte das empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público, de violações de segurança ou perdas de integridade ocorridas nas suas redes e serviços.

Sem prejuízo do cumprimento dos deveres de colaboração previstos no artigo 29º, a NOS reforça o entendimento de 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.

Por último, a NOS entende que os elementos solicitados nas alíneas a) ("todos os colaboradores envolvidos em cada fase da auditoria"), b) ("identificação dos seus fornecedores relevantes") e c) ("todos os colaboradores-chave") do nº1 do artigo 31º devem ser ajustados, de forma a que os mesmos não sejam de disponibilização obrigatória na fase de pré-auditoria e/ou que seja acautelada a possibilidade de revisão destes elementos em fases posteriores.

3. Conclusão

Em resumo, não obstante a evolução positiva verificada entre o primeiro e o segundo projeto de Regulamento, que se reconhece e saúda, a NOS entende que o atual projeto de regulamento inclui medidas que devem ser revistas ou eliminadas.

Para este efeito, as propostas da NOS, podem ser sintetizadas da seguinte forma:

i. A ANACOM deve ponderar a eliminação de medidas específicas que sejam redundantes com os objetivos de segurança, nomeadamente os requisitos da gestão dos riscos
i. O cumprimento dos níveis de sofisticação associados aos objetivos de segurança deve ser faseado, mais especificamente com a definição de um patamar de 80% do âmbito de cumprimento do nível 1 em 18 meses e do nível 2 em 36 meses
ii. Deve ser reavaliada a inclusão de todos os ativos dos clientes relevantes na classe de ativos A, assim como as obrigações de informação específicas para estes clientes em caso de ocorrências com impacto significativos
iii. O prazo previsto para implementação dos procedimentos de gestão de tráfego deve manter-se nos termos propostos na primeira versão do regulamento, sendo a implementação desta obrigação não é de forma alguma comportável com o prazo de 80 dias proposto
iv. Os requisitos associados ao Plano e Relatório Anual de segurança devem ser simplificados e ajustados de forma a que estas obrigações de complicação documental sejam proporcionais aos objetivos pretendidos, com o Plano de segurança a ser limitado à Política de Segurança e com a eliminação de requisitos a serem incluídos no Relatório anual
v. A ANACOM deve reavaliar a alteração empreendida ao prazo de publicação dos incidentes de segurança ao público, mantendo o atual prazo de 4 horas úteis
vi. As medidas de segurança impostas devem 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
vii. O objeto das obrigações previstas deve estar limitado à vertente de continuidade da prestação dos serviços e aos principais serviços de comunicações eletrónicas

viii. Deve ser prevista a possibilidade de as empresas que integram o mesmo Grupo poderem dar cumprimento às obrigações previstas individualmente ou de forma integrada

ix. A ANACOM deve proceder a uma inequívoca clarificação sobre o papel dos operadores nos domínios de segurança, em particular no que respeita a matérias de planeamento civil de emergência dos planos de emergência de proteção civil e da segurança interna

x. A partilha de informação deve ser substituída pela consulta dos dados sensíveis por parte de elementos da ANACOM, devidamente credenciados e habilitados, diretamente nas instalações dos operadores

xi. Finalmente, deve ser eliminada a obrigação de rotatividade das auditoras, sob pena de a exigência prescrita limitar de forma injustificada a escolha de uma empresa