APRITEL
ASSOCIAÇÃO DOS OPERADORES
DE COMUNICAÇÕES ELETRÓNICAS

Resposta da APRITEL à consulta pública da ANACOM sobre o 2º Projeto de Regulamento relativo à Segurança e à Integridade das Redes e Serviços de Comunicações Eletrónicas

I. Introdução

(1) A presente consulta pública decorre sobre um projeto de regulamento que tem o seu enquadramento na transposição da Diretiva 2009/140/CE pela Lei n.º 51/2011, de 13 de setembro, que veio alterar a Lei das Comunicações Eletrónicas (Lei n.º 5/2004, de 10 de fevereiro, na sua redação em vigor, adiante também designada 'LCE'), cometendo à ANACOM competências específicas para adotar regulamentação em matéria da segurança e integridade das redes e serviços.

(2) Num primeiro momento, por decisão de 12 de dezembro de 2013 (modificada em 8 de janeiro de 2014), a ANACOM concretizou as obrigações de notificação e de divulgação ao público de violações de segurança ou perdas de integridade com impacto significativo no funcionamento das redes e serviços.

(3) Num segundo momento mais recente (decisão de 4 de agosto de 2016), a ANACOM aprovou o *início do procedimento de elaboração de um regulamento relativo à segurança e integridade das redes e serviços*, para o que recolheu primeiros contributos, tendo depois aprovado por decisão de 29 de dezembro de 2016 o projeto de regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas, então submetido consulta (adiante, designado por 1.º projeto).

(4) A APRITEL, enquanto Associação dos Operadores de Comunicações Eletrónicas, respondeu a esta consulta pública e teve a oportunidade de detalhar, em reunião presencial com a ANACOM, as suas preocupações.

(5) Entendeu a ANACOM, em face das preocupações plasmadas nas quase duas dezenas de respostas recebidas a esta consulta pública, proceder à elaboração de um segundo projeto de regulamento e à sua submissão a novo procedimento

regulamentar e procedimento geral de consulta (adiante, o 2.º projeto) por decisão de 6 de julho de 2018.

(6) A APRITEL vem neste contexto responder à consulta sobre o segundo *Projeto de Regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas*, agrupando os seus contributos em 'comentários gerais' e 'comentários específicos', nos parágrafos seguintes, e para os quais desde já respeitosamente se pede a melhor atenção dessa Instituição.

II. Comentários Gerais

(7) A primeira observação geral que se oferece fazer sobre este 2.º projeto é a de que houve uma evolução positiva que deu relevância a parte importante dos contributos construtivos apresentados pela APRITEL em resposta à consulta pública que incidiu sobre o 1.º projeto.

(8) É de assinalar que para esta segunda versão do regulamento a ANACOM tomou em total consideração a necessidade de alinhamento deste normativo com as recomendações da ENISA, o que se afigurava imperioso. E também optou pela metodologia de definição de *objetivos* de segurança, ao invés das próprias *medidas operacionais* tendentes a alcançar esses objetivos.

(9) Com efeito, essa metodologia não deixava aos operadores a possibilidade de adotar as melhores medidas operacionais para a sua realidade individual.

(10) Refira-se também que a 1.ª versão impunha exigências de classificação de ativos, de cadastro e de documentação extremamente complexas e dificilmente praticáveis.

(11) Este 2.º projeto impõe o *nível 2 de sofisticação* para todos os objetivos e 11 medidas adicionais, aparentemente simplifica as exigências de classificação de ativos, cadastro e documentação e dá algum grau de liberdade aos operadores para adotarem as medidas operacionais e de implementação.

(12) Há, portanto, uma evolução geral positiva. Contudo, este 2.º projeto continua a levantar algumas preocupações importantes para as quais se pretende sensibilizar essa Instituição.

III. Comentários Específicos

Objeto (artigo 1.º)

(13) No âmbito das competências específicas cometidas à ANACOM, e que justificaram a elaboração deste projeto de regulamento, está a fixação de medidas adequadas para garantir a integridade das respetivas redes de maneira a assegurar a continuidade da prestação dos serviços que se suportam nas referidas redes, devendo para o efeito ser tido em consideração o disposto nos artigos 54.º-A, 54.º-C, n.º 1, e 54.º-D da Lei das Comunicações Eletrónicas (adiante, 'LCE').

(14) No n.º 2 do artigo 54.º-A é referido que as empresas que prestam serviços de comunicações eletrónicas devem adotar as medidas adequadas a garantir a integridade das respetivas redes de maneira a *assegurar a continuidade da prestação dos serviços que se suportam nas referidas redes*.

(15) Logo, julga-se imperioso dever prevalecer o entendimento, que a APRITEL teve já a oportunidade de expressar, de que o âmbito de aplicação das medidas técnicas e de execução, os requisitos adicionais e o processo de notificação de incidentes devem ser circunscritos à matéria relativa a disponibilidade de serviços e restritos a situações que acarretem interrupção de serviços de comunicações eletrónicas.

(16) Contudo, a ANACOM não clarifica quais os serviços de comunicações eletrónicas que devem ser abrangidos pelas medidas adotadas. No Relatório da consulta pública sobre o Projeto de regulamento de julho de 2018 indica-se mesmo que não se pode "limitar, em geral e a priori, o âmbito de aplicação deste projeto".

(17) Dificilmente se pode aceitar esse entendimento, já que desta indefinição resulta para os operadores, sujeitos de Direito, numa situação de indefinição do âmbito da previsão normativa e das respetivas consequências jurídicas, que são da maior importância. Insiste-se pois em que a ANACOM delimite o âmbito destas normas.

(18) Em concreto, o objeto a que as mesmas se dirigem devem ser os serviços de comunicações tidos como mais importantes para os cidadãos, a saber, os serviços de voz e de dados, fixos e móveis, e os serviços de televisão paga.

Âmbito (artigo 2.º)

(18) A obrigação de assegurar o cumprimento destas medidas de segurança deve restringir-se a condições normais de funcionamento e a situações extraordinárias devidamente elencadas, no sentido de que não tem cabimento os operadores serem obrigados a cumprir obrigações de segurança em cenários como sismos, incêndios e outras catástrofes naturais, em que pode ser impossível o cumprimento destas obrigações, sobretudo da obrigação de continuidade da prestação dos serviços, já que as redes e serviços podem ser afetadas independentemente da cabal adoção de todas as medidas preventivas.

(19) Aliás, em cenários de catástrofes nenhuma empresa ou entidade privada ou pública (com exceção talvez das entidades públicas cuja missão seja precisamente a de lidar com esse tipo de situações) conseguirá razoavelmente assegurar o mesmo nível de proteção. Portanto, o texto do 2.º projeto deve ser ajustado no sentido de flexibilizar o cumprimento das medidas de segurança e dos procedimentos exigidos pelo menos em situações como as descritas nas subalíneas v) e vi) da alínea b) do n.º 1 do artigo 2.º.

(20) Neste mesmo sentido, deve ser eliminada a alínea b) do SO 9 Segurança física e ambiental, que obriga os operadores a:

> "[d]efinir, aprovar e manter procedimentos de proteção e de preservação dos ativos de um modo adequado à evolução das condições climáticas da região e dos riscos de desastre natural ou de outros fenómenos extremos, incluindo tempestades, deslizamentos de terras, cheias, tornados, incêndios florestais, sismos ou maremotos."

(21) Note-se aliás que esta medida <u>não faz parte das medidas previstas pela ENISA</u>. Se é certo que é natural os reguladores nacionais poderem, em certa medida, proceder a adaptações das regras comuns aos contextos nacionais específicos, nesta matéria não se descortina no contexto português nenhum fator diferenciador que justifique um desvio às normas comuns aos mercados.

(22) A diversidade de situações jurídicas em que se encontram os ativos justifica que se explicite que a sujeição às obrigações de segurança está limitada exclusivamente aos ativos que são <u>propriedade plena</u> ou estão <u>sob a gestão exclusiva</u> dos operadores.

(23) Por exemplo, existem constrangimentos para assegurar o cumprimento destas obrigações em equipamentos localizados nas instalações dos clientes quando estes dois requisitos – propriedade ou gestão exclusiva pelo operador – não se verifiquem. É o caso de um *router* "privado" na habitação de um cliente residencial. E mesmo quando o equipamento seja juridicamente pertença do operador e por este remotamente gerido, o facto de se encontrar nas instalações do cliente e de não estar por conseguinte na posse do operador, não permite garantir que o mesmo não seja acedido indevidamente.

Meios electrónicos (Artigo 5.º)

(23) A partilha por meios eletrónicos de informação sensível, classificada como confidencial ou secreta, aumenta os riscos sobre a segurança dessa mesma informação, caso o referido "sistema de informação" não possua medidas de segurança robustas na transmissão, acesso e armazenamento de informação. Este risco pode ainda ser acrescido se a informação for partilhada por email, no caso de o sistema de partilha de informação não estar (ainda) disponível.

(24) Caso um tal sistema não esteja disponível, a partilha ou transmissão 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.

Medidas técnicas de segurança (Artigo 7.º)

(25) Reconhece-se o propósito de incorporar neste novo sentido provável de decisão a proposta para substituir algumas medidas prescritivas por um modelo de fixação de objetivos de segurança, ou *Security Objective* (adiante designados por 'SO').

(26) Contudo, para além do cumprimento dos 25 SO, a ANACOM pretende impor o cumprimento de 11 medidas específicas. A verdade é que algumas destas 11 medidas específicas já se encontram de alguma forma cobertas pelos SO, conforme se pode verificar na tabela infra.

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

(27) Nos comentários seguintes a cada um dos artigos do texto do regulamento com medidas específicas são abordadas estas redundâncias, assim como outros aspetos que justificam a sua revisão ou mesmo eliminação.

(28) Julga-se que a satisfação dos níveis de sofisticação deve ser faseada, sugerindo-se a consideração de patamares de progressão de 80% do âmbito de cada medida. O cumprimento do regulamento constituirá um ónus significativo para os operadores que só por isso redundará numa barreira à entrada e à

expansão de redes e serviços de comunicações electrónicas. Por esse motivo defende-se uma estratégia de progressão por etapas no cumprimento dos objetivos com medidas novas ou para elevação do nível de sofisticação das medidas já em execução pelos prestadores, conferindo-lhes tempo e flexibilidade para se adaptarem e incorporarem aprendizagens e diluindo assim os custos de implementação e adaptação a este regulamento. Demonstrativo da pertinência desta flexibilidade é a circunstância de alguns objetivos poderem até já estar a ser assegurados por medidas de grau 3, sem que tenham tido que ser implementadas medidas dos graus 1 ou 2.

(29) Uma abordagem 'passo-a-passo' é perfeitamente razoável e prudente e não coloca em causa o objetivo final que é o de ter, no prazo de alguns anos, um nível de sofisticação elevado no cumprimento dos SO.

(30) A ANACOM, na sua análise, não procedeu a uma avaliação de impacto dos custos e benefícios associados à satisfação direta de exigências do nível 2 ou superior *versus* o cenário de se começar pelo nível 1 evoluindo gradualmente para os níveis superiores, solução esta que se afigura mais consentânea com o princípio da proporcionalidade e que deve estar contemplada.

Classificação de ativos (Artigo 8.º)

(31) Há uma aparente simplificação do cadastro e da classificação de ativos. Porém, a fusão das anteriores categorias A e B mantém na prática a complexidade destas regras. Não é apresentada qualquer explicação para se ter agregado numa única classe (A) as anteriores classes A e B do primeiro projeto em consulta. Também se questiona a razão para o significativo alargamento dos critérios de classificação dos ativos da nova classe A.

(32) A este respeito, o n.º 2 do artigo 8.º merece uma nota importante. A utilização da conjunção alternativa "ou" para o segundo critério de classificação "[… **ou** a área geográfica afetada possa ser igual ou superior a 2.000 km2"] (sublinhado nosso) faz com que todos os equipamentos cuja abrangência funcional seja superior a uma área geográfica equivalente ao Distrito do Porto, por exemplo, caiam na Classe A mesmo que abranjam menos de 100.000 Clientes. Não parece que esta seja a intenção da ANACOM. A sugestão da APRITEL é a de que o critério da área geográfica apenas seja aplicado subsidiariamente, ou seja, quando não

for possível calcular o n.º de acessos afetados, à semelhança do que se lê no artigo 21.º, n.º 3, e):

> *"O critério relativo à área geográfica afetada só deve ser aplicado caso o critério relativo ao número de assinantes ou de acessos afetados seja inaplicável ou, no caso concreto, fundamentadamente impossível de determinar ou estimar."*

(33) Relativamente aos ativos da classe A, sobre os quais recai grande parte das obrigações, a APRITEL considera que os mesmos não devem ser alargados aos *clientes relevantes* seguintes:

i. *SIRESP e RNSI* - Estas entidades, pela sua natureza e função de atuação em situações de emergência ou crise, devem possuir as suas próprias capacidades de resiliência para assegurar a continuidade da prestação dos seus serviços;

ii. *Operadores de serviços essenciais (por exemplo, empresas do setor de distribuição de energia, empresas do setor dos transportes, prestadores de cuidados de saúde, instituições bancárias, prestadores de infraestruturas digitais, etc.) ou operadores de infraestruturas críticas (por exemplo, empresas do setor da energia e dos transportes)* - São habitualmente empresas que possuem redes de distribuição próprias e uma presença nacional em todo o País. Assim, se considerarmos todos os ativos de rede (incluindo eventuais equipamentos do cliente sob gestão do operador) que suportam estes clientes, estaríamos a considerar que grande parte dos ativos de um operador seriam considerados ativos de classe A, o que desvirtuaria por completo a segmentação de criticidade que se pretende entre os ativos das classes A, B e C e, adicionalmente, acarretaria ainda maior complexidade para a gestão de toda a informação e caracterização que o regulamento exige para os ativos de classe A.

iii. *Outras entidades que a ANACOM poderá designar* - Não é razoável que possam ser designados 'clientes relevantes' no prazo de apenas 5 dias úteis e sem a identificação de critérios mais específicos.

(34) A alínea e) do nº 3 do artigo 8º determina que devam ser considerados os ativos que foram identificados à ANPC no âmbito do processo de identificação de infraestruturas críticas. Este artigo cria muita imprevisibilidade e coloca nas

mãos de terceiros a identificação dos ativos críticos dos operadores de redes e serviços. Deve caber aos operadores decidir quais os ativos essenciais ou críticos para assegurar o cumprimento dos objetivos e obrigações de segurança que lhes sejam fixadas no âmbito invocado pela ANACOM.

(35) A definição de ativo da classe B (Artigo 8.º, n.º 4) é ambígua e cria espaço para interpretações diferentes, pelo que se afigura conveniente detalhar o que se considera "impacto negativo grave":

> "*Um ativo deve ser classificado na classe B se, em resultado de perturbação do seu funcionamento, cause ou possa vir a causar um impacto negativo grave na segurança das redes e serviços ou na sua continuidade, exceto quando, nos termos previstos nos números anteriores, deva ser classificado na classe A."* (Sublinhado nosso.)

Inventário de ativos (Artigo 9.º)

(36) O processo de inventário continua a ser muito complexo, impondo um número excessivo de requisitos, e é por isso demasiado oneroso, sem vantagens para os objetivos de segurança das redes prosseguidos pelo regulamento.

(37) Mantém-se a necessidade de incluir na comunicação à ANACOM dados como coordenadas geográficas de localização e a identificação das respetivas entidades detentoras ou gestoras dos locais (cfr. artigo 9.º, n.ºs 2 e 5). Estes elementos constituem informação muito sensível, cuja confidencialidade não se deve sujeitar a riscos que não estejam estritamente justificados por critérios de proporcionalidade entre o objetivo pretendido com a sua comunicação ao regulador e o risco aumentado associado à partilha de informação.

(38) Os atributos beneficiarão com uma revisão e simplificação. Os critérios de classificação (atributos) devem limitar-se ao impacto medido em assinantes/acessos (ou área geográfica) impactados por uma interrupção do serviço ou outros que sejam entendidos pelos operadores com caracterizadores da criticidade de um ativo. A caracterização do ativo no inventário deve ser deixada ao critério do operador, e deve utilizar o modelo de dados já utilizado pelo operador, a fim de dispensar custos de implementação adicionais não justificados e supérfluos (e, logo, desproporcionais).

(39) Neste modelo de flexibilidade, os atributos constantes do regulamento devem poder ser vistos como exemplificativos.

(40) Os ativos da Classe C - *Ativos Não Críticos* - não devem fazer parte do inventário para efeitos deste regulamento. Por conseguinte, o número 2 do artigo 9.º deve excluir estes ativos do âmbito de aplicação da obrigação de inventariação, com a informação associada.

(41) O Artigo 9.º, n.º 5, merece a total oposição dos operadores, porquanto a informação que se pretende seja transmitida à ANACOM é extremamente sensível e, não só não está garantida de acordo com padrões apropriados a sua absoluta confidencialidade (por exemplo, em sistemas de armazenamento, regimes de autorização e registos de acesso mediante credenciais e 'logs' de acesso…), como nem sequer se apresenta o objetivo de acesso a esta informação pela ANACOM. Existem riscos de quebra de segurança pelo simples facto de se estar a transmitir a informação e a duplicá-la num qualquer sistema na ANACOM. As auditorias da ANACOM devem certificar a existência e atualização do inventário e isso é tudo quanto a ANACOM deve necessitar saber. Adicionalmente, A ANACOM poderá, com um pedido fundamentado, consultar o inventário de ativos nas instalações do operador.

Requisitos da gestão dos riscos (Artigo 10.º)

(42) A fixação destes requisitos é redundante com a fixação de SO de nível 2. Afigura-se pertinente, isso sim, 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. Mas não se afigura correto rever a própria metodologia de gestão do risco, pois esta é basilar a toda a análise de risco e classificação de ativos.

(43) A APRITEL sugere por isso a eliminação deste artigo 10.º do regulamento.

Exercícios (Artigo 12.º)

(44) Ainda que a periodicidade tenha sido alargada, 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.

(45) Por outro lado, A palavra "bianual" presta-se a ambiguidades porque também tem o significado de "2 vezes por ano". Sugerimos que se coloque por extenso "de *x* em *x* anos". Mesmo assim, uma periodicidade de dois anos para os exercícios poderá ser excessiva, pelo que se sugere o alargamento para três anos.

Clientes relevantes (Artigo 13.º)

(46) De acordo com o artigo 21.º, n.º 5, são 'clientes relevantes' os seguintes:

a) O SIRESP;

b) A RNSI;

c) O SRPCBA;

d) A partir da data da notificação da sua identificação, pela ANACOM, às empresas:

> *i) Os operadores de serviços essenciais a identificar no âmbito da aplicação do diploma de transposição da Diretiva (UE) n.º 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União;*
>
> *ii) Os proprietários ou operadores de infraestruturas críticas designadas ao abrigo do disposto no Decreto-Lei n.º 62/2011, de 9 de maio, e na demais legislação aplicável;*

e) Outras entidades a identificar pela ANACOM, devidamente notificadas às empresas com uma antecedência mínima de cinco dias úteis.

(47) Os operadores prestam de forma voluntária e transparente informações detalhadas aos clientes, em canais próprios e nos moldes adequados às suas necessidades específicas, estando contemplados mecanismos contratuais de estabelecimento de requisitos específicos de comunicação perfeitamente aptos a ir ao encontro da informação considerada relevante e valorizada pelo cliente, e que por isso melhor responde às suas necessidades específicas. Esta

flexibilidade tem vantagens sobre a estipulação genérica de obrigações acrescidas a um conjunto específico de clientes.

(48) Considerando que a ANACOM é notificada nos termos do artigo 22.º, não fica claro o motivo para a ANACOM ser informada das medidas implementadas com impacto em clientes específicos antecipadamente à receção da notificação final prevista nos n.ºs 8 e 9 do artigo 22º.

(49) O âmbito de aplicação deste regime fica sujeito ao alargamento previsto aos operadores de serviços essenciais, proprietários ou operadores de infraestruturas críticas ou a qualquer entidade que a ANACOM designe através de notificação com 5 dias úteis de antecedência. Este alargamento vai envolver empresas de setores como o financeiro, a saúde ou de abastecimento de águas, que passam a ter desta forma um tratamento diferenciado em matérias de segurança.

(50) A ANACOM está a impor este ónus aos operadores sem que no sentido inverso os operadores possam beneficiar de análogo tratamento preferencial correlacionado, assim desprotegendo o setor face a outros setores com reguladores próprios.

(51) A APRITEL considera que caberá àquelas entidades identificar o seu grau de dependência das redes e serviços de comunicações eletrónicas e, em conformidade, contratar com os operadores as soluções adequadas de resiliência e os níveis apropriados de QoS.

Ponto de contacto permanente (Artigo 15.º) e Equipa de resposta a acidentes (Artigo 16.º)

(52) As alíneas c) e d) do artigo 15.º do regulamento impõem aos operadores obrigações de “construção e atualização de informação de situação integrada no contexto de uma violação de segurança ou perda de integridade com impacto significativo ou da ativação do planeamento civil de emergência ou de plano de emergência da proteção civil” e de participação em planos de emergência e proteção civil. Ora, os operadores não têm, à data, como saber qual o seu papel num e noutro âmbito. O regulamento deve, imperiosamente, prever que estas

obrigações ficam condicionadas ao envolvimento dos operadores na definição destes planos e à obtenção da devida informação.

(53) Note-se que, contrariamente ao referido 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 (pág. 11), continuam a não ser claras as fronteiras entre as competências das várias entidades em matéria de planeamento civil de emergência e de proteção civil e da segurança interna. Assim, reitera-se o pedido para que a ANACOM, como regulador setorial proceda à devida clarificação do papel das empresas e entidades competentes, de forma a garantir que todas as entidades conhecem de forma inequívoca o seu papel e responsabilidades e possam dar cumprimento às suas obrigações nos domínios de segurança, incluindo as situações de emergência.

(54) Quanto às equipas de resposta a incidentes, os operadores devem ter a flexibilidade de adaptar meios alocados à resolução das violações de segurança ou perda de integridade – ou seja os elementos não deveriam ser estanques e por isso incluídos na lista de colaboradores-chave a ser incluída na alínea d) do n.º1 do artigo 17.º, nem ser objeto do procedimento descrito no n.º 3 do artigo 17.º de demonstração dos comprovativos de que se encontram devidamente mandatados, nos termos legalmente previstos, para representar a empresa no exercício da função.

(55) A APRITEL considera que o n.º 3 deste artigo configura uma intervenção excessiva na organização e vida interna dos operadores e deve, por conseguinte, ser eliminado. A equipa de resposta a incidentes de segurança prevista neste artigo não deve ter que integrar, necessariamente, o sistema de resposta a incidentes de segurança da informação nos termos a determinar ao abrigo do disposto na alínea d) do n.º 2 do artigo 2.º-A da Lei das Comunicações Eletrónicas.

Plano de Segurança (Artigo 17.º)

(56) O artigo 7.º do regulamento prescreve na alínea a) como objetivo 1 a existência de uma política de segurança. O artigo 17.º deve limitar-se ao fixado na alínea a) com exclusão do que consta das alíneas seguintes, porquanto a fixação desta

informação num suporte acessível por várias entidades cria uma situação de risco e vulnerabilidade sobre as próprias redes e serviços.

(57) Por outro lado, as preocupações subjacentes às alíneas b) a d) do artigo 17.º já 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*). Sendo redundantes e geradoras de riscos, estas obrigações devem ser eliminadas.

Relatório anual de segurança (Artigo 19.º)

(58) Compreendendo embora a pertinência da elaboração de um relatório anual de segurança, nem por isso deixa de se fazer notar alguns aspetos que se julga merecerem ser melhorados. Com efeito, houve alguma simplificação nas obrigações de documentação, mas aumentaram as exigências ao nível do relatório anual.

(59) A disponibilização de estatísticas trimestrais dos incidentes "sem impacto significativo" (alínea b)) não deve, por definição, ser obrigatória: estes incidentes "sem impacto significativo" não são relevantes face às regras e patamares definidos no regulamento. Com efeito, nesta categoria estariam interrupções de serviços que tivessem afetado apenas um único cliente e num período residual.

(60) Quanto ao programa de exercícios (alínea d)) deve ser opcional a indicação do programa de exercícios previstos para ano civil seguinte, sendo apenas obrigatório indicar o programa de exercícios do ano a que respeita o relatório. Esta proposta justifica-se pelo facto de poder não ser exequível, com a antecipação pretendida, a identificação dos ativos e serviços que vão ser incluídos no âmbito dos testes.

(61) O envio dos elementos solicitados ao abrigo da notificação de incidentes de segurança e perdas de integridade (alínea c)) fornece à ANACOM os elementos necessários à realização de uma análise agregada dos incidentes com maior impacto, com a mais-valia de o Regulador dispor dos dados de todos os operadores presentes no mercado, pelo que se podem dispensar os operadores dessa tarefa.

Circunstâncias associadas às obrigações de notificação de incidentes (Artigo 21.º)

(62) As entidades mais bem posicionadas para comunicar as violações de segurança e perdas de integridade que envolvam entidades críticas para a segurança nacional, conforme se dispõe nas alíneas b) e f) do número 2 do artigo 21.º são as próprias entidades, pelo que deverão ser estas a assegurar essa comunicação.

(63) O número 5 deste artigo confere um grau de discricionariedade ao Regulador dificilmente compatível com o princípio da legalidade, atentatório do princípio da segurança e certeza jurídicas e deve, por conseguinte, ser remetida a possibilidade de designar "outras entidades" para norma habilitante adequada, à semelhança, por exemplo, do constante das subalíneas i) e ii) da alínea d) do mesmo número. Ademais, um tão exíguo prazo de antecedência, de apenas 5 dias úteis apenas, sem audiência prévia, é arbitrário, desproporcional e por isso de legalidade muito duvidosa.

Formato e procedimentos (Artigo 22.º)

(64) O apuramento concreto das freguesias e respetivos concelhos afetados por violações de segurança ou perda de integridade é um processo complexo e moroso, particularmente quando são afetados determinados segmentos de rede ou tecnologias. Existem importantes constrangimentos para garantir o pleno cumprimento do n.º 7 do artigo 22.º, sobretudo no prazo de duas horas após o fim da ocorrência. Assim, a indicação concreta das zonas afetadas deverá ser limitada à notificação final e deverá manter-se o regime atual de localização ao nível do concelho e não da freguesia.

Notificação ao público (Artigo 24.º)

(65) Problema idêntico ao referido a propósito do n.º 7 do artigo 21.º se coloca em sede de aplicação do artigo 24.º, nº 1, alínea a), subalínea ii), em que é exigida "a indicação da zona ou das zonas que, em resultado das violações de segurança ou das perdas de integridade ocorridas, se encontram afetadas,

desagregadas ao nível da freguesia, se possível de modo gráfico sobre um mapa de Portugal".

(66) Esta informação ao nível da freguesia implicaria custos elevados de Sistemas de Informação e muitas vezes não é viável ou é complexa de determinar em alguns cenários de incidente ou em certos segmentos de rede ou tecnologias, pelo que se propõe que esta obrigação seja retirada do regulamento.

(67) No n.º 1, alínea c) indica-se que o operador deve "disponibilizar a informação logo que possível, no prazo máximo de uma hora após a notificação inicial à ANACOM". Esta alteração é surpreendente, constituindo um retrocesso no regime vigente, uma vez que este prazo de 1 hora foi inicialmente veiculado no sentido provável de decisão de 22 de dezembro de 2011, mas alterado, na sequência das preocupações e constrangimentos demonstrados pelos operadores, para justificar as 4 horas úteis.

(68) Salienta-se que no correspondente relatório a ANACOM justificou esta 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.

(69) Se assim fosse os operadores teriam que ter em permanência equipas de mera comunicação 24 horas/7 dias para tratarem da publicação desta informação. Note-se que a comunicação feita em *site* aos clientes não é uma mera cópia da notificação à ANACOM. Trata-se de comunicação com clientes, que usa uma linguagem própria, adequada ao contexto e de acordo com a política de comunicação do operador, e que, por isso é aprovada por equipas diferentes da equipa técnica, que é quem assegura as notificações à ANACOM.

(70) A APRITEL, reiterando os argumentos então aduzidos na consulta que resultou na deliberação de 12 de dezembro de 2013, que se mantêm inteiramente pertinentes, considera importante eliminar esta alteração de prazo.

Auditorias (Artigos 25.º a 33.º)

(71) Uma primeira nota a fazer a respeito dos critérios que devem ser acautelados na realização de auditorias é a de que a sua viabilidade está condicionada à

existência, no mercado, de empresas auditoras com o nível de experiência propugnado.

(72) Não existem no mercado muitas auditoras especializadas, pelo que se aconselha a eliminação do n.º 3 do artigo 28.º, segundo o qual "*[a]s empresas devem assegurar a rotatividade na escolha das auditoras, de modo a que a mesma auditora não realize mais do que duas auditorias consecutivas*"), minimizando assim o risco de não se encontrarem empresas que cumpram os critérios fixados. Não é realmente imprescindível que mude a empresa auditora. O que é pertinente é que as equipas de auditores mudem, podendo a empresa ser a mesma. A generalidade das auditoras tem uma rotatividade dos colaboradores envolvidos em processos de auditorias recorrentes, pelo que poderá estar mais facilitado o preenchimento deste requisito.

(73) Qualquer colaborador da ANACOM que tenha intervenção nos processos de auditoria deverá estar sujeito aos mesmos 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.

(74) Sem prejuízo do cumprimento dos deveres de colaboração previstos no artigo 29.º, 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.

(75) Não parece justificar-se a realização das auditorias de 2 em 2 anos, com os custos que têm associados. A APRITEL propõe uma periodicidade de 3 anos.

(76) No artigo 31.º, as alíneas a) e e) são excessivas face aos elementos da alínea f), não se justificando enviar mais do que o Plano de Auditoria, conforme descrito nesta última alínea, para que o Regulador, querendo, possa acompanhar a realização da auditoria. Com efeito, o processo pode beneficiar com uma redução da carga burocrática.

(78) Finalmente, suscita as maiores reservas o envio à ANACOM de informação com a identificação de fornecedores relevantes em matéria de segurança ou a lista de colaboradores-chave.

Prazos (Artigo 35.º)

(79) O n.º 2, alínea c), subalínea ii) do artigo 35.º concede um prazo de apenas 80 dias para o operador, "[c]aso aplicável, adotar os procedimentos de controlo da gestão excecional de tráfego de acesso à Internet, nos termos previstos no artigo 11.º". A adoção dos procedimentos contemplados no artigo 11.º exige desenvolvimentos complexos. Por isso, adequadamente, o primeiro projeto contemplava para a implementação destes procedimentos o prazo de 18 meses previsto na alínea d) do número 2 do artigo 35.º para outros procedimentos que se consideram dos mais morosos, como sejam, a conclusão da classificação e inventariação dos ativos, a adoção de uma série de importantes medidas de segurança ou a conclusão da elaboração do plano de segurança nos moldes contemplados no regulamento.

(80) A implementação destes procedimentos em 80 dias não é viável, inclusivamente porque são exigidos desenvolvimentos por parte dos fornecedores, cujos *timings* escapam à capacidade de controlo dos operadores.

(81) Solicita-se assim que seja mantido o prazo de implementação desta obrigação de 18 meses.

(82) O prazo de 18 meses previsto na subalínea ii) da alínea d) do n.º 2 do artigo 35.º deste segundo projeto para a adoção de "*todas as restantes medidas de segurança aplicáveis nos termos do previsto no Título II e no Anexo ao presente regulamento, sem prejuízo do disposto nos n.º 3 e 5 do presente artigo"* encurtou para metade o prazo que, para a mesma matéria, estava previsto no primeiro projeto de regulamento, e que, com toda a razoabilidade, permitia mitigar um pouco o impacto operacional e financeiro inerente à implementação deste regulamento. Não se entende um desvio tão significativo (um corte para metade), desconsiderando os equilíbrios financeiros e operacionais das empresas, para o que não se vislumbra justificação na existência de alguma premência de maior na aceleração das medidas ali previstas. Requer-se assim a melhor consideração para estas preocupações e, nesse sentido, a reposição do prazo de 36 meses do primeiro projeto.