[redacted]

From: [redacted]
Sent: 14 de março de 2017 23:43
To: regulamento.seguranca@anacom.pt
Cc: [redacted]
Subject: APRITEL | Consulta sobre o projeto de regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas
Attachments: Projeto Regulamento Segurança de Redes_VF.PDF; Projeto de Regulamento Segurança _ Anexo I.PDF

Exmos. Senhores,

Vimos pelo presente enviar a resposta da APRITEL à consulta pública sobre o projeto de regulamento relativo à segurança e integridade das redes e serviços de comunicações eletrónicas.

Ficando ao dispor para qualquer informação adicional necessária, despeço-me,

Com os melhores cumprimentos,

[redacted]

APRITEL

[redacted]

Largo Rafael Bordalo Pinheiro, n.º 16 (ao Chiado) – Escritório 1.03
1200-369 Lisboa

[redacted]

Ref.: SecGerCrsp_R674/2017

Consulta sobre o Projeto de Regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas

Na sequência do lançamento da consulta sobre o Projeto de Regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas, vem a APRITEL – Associação dos Operadores de Comunicações Eletrónicas enviar os seus comentários, que adiante se sistematizam como 'comentários gerais' e 'comentários específicos'.

I - COMENTÁRIOS GERAIS:

1. Fundamentação e ausência de uma análise de impacto

As obrigações constantes do Projeto de Regulamento devem ser proporcionais quanto às restrições ou intrusões que impõem na esfera privada das empresas, quanto à onerosidade das medidas impostas e quanto ao impacto negativo que a execução de certas medidas pode ter na própria continuidade do serviço.

O artigo 54.º- A, n.ºs 1 e 2, da LCE (que resulta da transposição da Diretiva 2009/140/CE de 25.11.2009) dispõe que:

> *1 - As empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público devem adotar as medidas técnicas e organizacionais adequadas à prevenção, gestão e redução dos riscos para a segurança das redes e serviços visando, em especial, impedir ou minimizar o impacte dos incidentes de segurança nas redes interligadas, a nível nacional e internacional, e nos utilizadores.*
>
> *2 - As empresas que oferecem redes de comunicações públicas são obrigadas a adotar as medidas adequadas para garantir a integridade das respetivas redes, assegurando a continuidade da prestação dos serviços que se suportam nas referidas redes.*

APRITEL – Associação dos Operadores de Comunicações Eletrónicas
Largo Rafael Bordalo Pinheiro, n.º 16 (ao Chiado) – Escritório 1.03, 1200-369 Lisboa
. Tel.: +351 213 550 911 • apritel@apritel.org • www.apritel.org • NIPC: 504 169 998

Deve, contudo, interpretar-se a lei nacional com o sentido e alcance pretendido pela Diretiva 2009/140, que aquela veio transpor, em particular no que resulta da leitura dos seguintes Considerandos:

> ***Considerando 44***
>
> *Tendo em conta que a aplicação com êxito de meios de segurança adequados não é um exercício pontual, mas um processo contínuo de execução, revisão e atualização, deverá exigir-se aos fornecedores de redes e serviços de comunicações eletrónicas que tomem medidas para proteger a sua integridade e segurança em função dos riscos avaliados, tendo em conta, na aplicação dessas medidas, o estado da técnica.*

Portanto, trata-se de um processo contínuo, em que os fornecedores de redes e serviços de CE tomam medidas em função dos riscos avaliados.

> ***Considerando 45***
>
> *Os Estados-Membros deverão prever um período adequado de consulta pública antes da aprovação de medidas específicas, a fim de assegurar que as empresas que oferecem redes de comunicações públicas ou prestem serviços de comunicações eletrónicas ao público tomem as medidas técnicas e organizacionais necessárias para gerir adequadamente os riscos para a segurança das redes e serviços ou para garantir a integridade das suas redes.*

Portanto deve ser dada às empresas latitude para adoção das medidas técnicas e organizacionais necessárias para gerir adequadamente os riscos para a segurança e garantir integridade das redes.

Mesmo a ANACOM refere ter uma preocupação com o impacto e a proporcionalidade das medidas face aos problemas e riscos, os quais justificariam o elevado grau de intervenção proposto. No parágrafo 7.º da Nota Justificativa do Regulamento, a ANACOM refere:

> *7. Na regulamentação das obrigações das empresas em matéria de segurança e integridade das redes e serviços, foram objeto de ponderação, por um lado, os custos a incorrer pelas empresas no cumprimento das suas obrigações e, por outro, os benefícios daí emergentes, os quais incluem não só a defesa dos interesses dos cidadãos e, em particular, dos utilizadores das redes e serviços, o suporte à continuidade da prestação de serviços relevantes à sociedade e*

APRITEL – Associação dos Operadores de Comunicações Eletrónicas
Largo Rafael Bordalo Pinheiro, n.º 16 (ao Chiado) – Escritório 1.03, 1200-369 Lisboa
. Tel.: +351 213 550 911 • apritel@apritel.org • www.apritel.org • NIPC: 504 169 998

aos cidadãos, a garantia do acesso aos serviços de emergência e, em geral, a promoção do desenvolvimento do mercado interno por via da melhoria da fiabilidade das redes e serviços, como também aqueles resultantes da prevenção de incidentes de segurança e do impedimento ou minimização do respetivo impacte.

Contudo, faltam evidências sobre alguns aspetos cruciais desta análise, nomeadamente:

- custos das medidas que se pretendem adotar - não se conhece nenhuma estimativa de custos da adaptação de procedimentos atuais ou adoção de processos adicionais face ao que já está implementado pelos operadores, que tenha sido considerada na preparação das medidas preconizadas no Projeto de Regulamento.

- estudos de impacto - também não foi prestada evidência da realização de uma adequada avaliação de impacto, indispensável à imposição de medidas com tão elevado nível de intrusão na esfera interna e organização das empresas; nem sequer se viu ser considerado que algumas medidas de testes podem; elas próprias, ter impacto negativo na continuidade da prestação do serviço;

- *benchmark* - também não são apresentados dados de *benchmark* como alternativa que permita aferir da proporcionalidade e razoabilidade das medidas propostas face às necessidades reais e objetivos prosseguidos.

- *Riscos e ameaças* - não se identificam os objetivos de segurança/integridade específicos, nem os riscos e ameaças considerados, que permitam às empresas aferir se os mesmos já estão atingidos através das medidas que já têm implementadas.

Nestas circunstâncias, a APRITEL solicita que o futuro regulamento seja precedido de uma avaliação de impacto *(impact assessement)*, e que sejam ponderados os impactos - administrativos, operacionais e financeiros - associados em face dos objetivos e benefícios identificados pela ANACOM. De igual modo, devem ser indicados os riscos e problemas identificados, e que justificam o grau de intervenção adotado. Apenas desta forma será possível garantir que a intervenção não descura os princípios de razoabilidade e proporcionalidade, assim como é eficaz e direcionada à resolução dos riscos e ameaças identificados.

APRITEL – Associação dos Operadores de Comunicações Eletrónicas
Largo Rafael Bordalo Pinheiro, n.º 16 (ao Chiado) – Escritório 1.03, 1200-369 Lisboa
. Tel.: +351 213 550 911 • apritel@apritel.org • www.apritel.org • NIPC: 504 169 998

2. Proporcionalidade

Complementarmente, destaca-se a interpretação desta Diretiva dada pela ENISA - *Guideline on Security measures for Article 4 and Article 13a Version 1.0 December 2014*

> ***"One size does not fit all**: Neither the high-level security objectives nor the detailed security measures should be seen as binding recommendations about which are appropriate security measures for providers to take. The reason is that the electronic communications sector is very diverse; large incumbents, small service providers, black fibre operators, virtual mobile network operators, ISPs offering only DSL, et cetera. In each setting the risks are different and it is up to the providers to assess the risks and decide which are appropriate security measures to take."*

Ou seja, atenta a redação dos preceitos legais e a interpretação dos mesmos feita pela própria ENISA, facilmente se conclui ser entendimento geral que nem todos os operadores têm a mesma dimensão ou nível de maturidade na sua rede, pelo que as medidas a implementar devem ter flexibilidade para se adaptarem a tais diferentes realidades, em cada contexto específico.

Considerando o contexto do nosso País, entende ainda a APRITEL que as medidas propostas são excessivas e muito intrusivas face aos riscos e ameaças a que as redes nacionais estão sujeitas, quer no plano geopolítico, quer do ponto de vista de catástrofes naturais, e, portanto, estão desenquadradas do quadro nacional, não deixando sequer margem aos operadores para definir os meios (medidas de execução) mais adequados aos objetivos pretendidos.

O Projeto de Regulamento não endereça também a posição dos grandes *carriers* globais com uma presença extremamente reduzida em Portugal que já cumprem outros e exigentes padrões de segurança. Trata-se de operadores que já adotam políticas internas de segurança, de auditoria e relatórios, à escala internacional. Não será viável impor obrigações paralelas com diferentes parâmetros para um mercado local onde esse *carrier* tem uma pequena operação. Também estes casos aconselham uma muito maior flexibilidade.

Os operadores estimam um impacto financeiro muito elevado do Projeto de Regulamento, na medida em que a implementação das medidas constantes do Projeto de Regulamento tem um impacto estrutural nas empresas, quer ao nível da rede, plataformas e serviços (em particular ao nível da Gestão de alterações), quer ao nível

APRITEL – Associação dos Operadores de Comunicações Eletrónicas
Largo Rafael Bordalo Pinheiro, n.º 16 (ao Chiado) – Escritório 1.03, 1200-369 Lisboa
. Tel.: +351 213 550 911 • apritel@apritel.org • www.apritel.org • NIPC: 504 169 998

dos recursos técnicos e humanos. Os custos das medidas contempladas no Projeto de Regulamento para o setor, já de si pesadamente onerado, devem ser avaliados também à luz da circunstância de que todos os operadores têm já implementadas medidas e políticas de segurança, pelo que as obrigações impostas pela ANACOM implicam uma duplicação ou substituição de procedimentos.

3. Âmbito

A APRITEL entende que as obrigações impostas no Projeto de Regulamento visam acautelar incidentes que afetem a continuidade dos serviços de comunicações eletrónicas e, portanto, os incidentes que implicam a interrupção desses mesmos serviços, considerando-se que não estarão no âmbito deste Regulamento os incidentes de segurança que comprometam, por exemplo, a confidencialidade das comunicações ou a proteção dos dados pessoais, temas estes, aliás, tratados em sede própria, nomeadamente através do Regulamento (UE) 2016/679, de 27 de abril de 2016 e da Lei n.º 41/2004, de18 de agosto, alterada pela Lei n.º 46/2012 de 29 de agosto.

O âmbito do Projeto de Regulamento deve assim estar limitado à garantia da continuidade e integridade das redes e serviços com o objetivo de minimizar a interrupção dos serviços de comunicações eletrónicas.

As referências e as obrigações associadas a planeamento civil de emergência e de segurança interna criam ambiguidade acerca das obrigações dos operadores neste âmbito e das entidades intervenientes, pelo que deveria ser, no mínimo, disponibilizada aos operadores informação clara sobre as ações em concreto que devem ser desenvolvidas pelos operadores e clara delimitação das competências das entidades intervenientes neste domínio.

4. Comparação internacional

A APRITEL obteve, via *Cullen International*, informação sobre a implementação de medidas de segurança e integridade de redes em Espanha, França, Itália, Bélgica, Reino Unido, Irlanda e Suécia, tendo-se concluído que as propostas avançadas pela ANACOM consubstanciam o regime mais exigente neste grupo de países analisados.

O regime sueco é o que mais se aproxima do regime preconizado pela ANACOM, mas com prazos de implementação mais dilatados e menos exigências de reporte. A APRITEL questiona em que medida os riscos identificados pela ANACOM são comparáveis com os que foram identificados pelo regulador sueco.

APRITEL – Associação dos Operadores de Comunicações Eletrónicas
Largo Rafael Bordalo Pinheiro, n.º 16 (ao Chiado) – Escritório 1.03, 1200-369 Lisboa
. Tel.: +351 213 550 911 • apritel@apritel.org • www.apritel.org • NIPC: 504 169 998

Nos restantes países, as medidas específicas não têm o detalhe e a abrangência do Projeto de Regulamento da ANACOM.

Em geral, estes regimes impõem obrigações genéricas de garantir a segurança e integridade das redes e das infraestruturas críticas e depositam no sentido de responsabilidade dos operadores a escolha e implementação das medidas mais adequadas para dar cumprimento àquelas obrigações. Por exemplo, o regulador irlandês afirma o seguinte:

> "*ComReg is aware that not all Operators are the same, with significant variations in customer base and product portfolios, which may result in different approaches to the management of risk-assessment*."

Em Portugal os fatores de risco são relativamente reduzidos, o que dificulta a justificação da imposição das medidas previstas no Projeto de Regulamento, as quais implicam elevados custos. Entende a APRITEL que, caso se adote um faseamento das medidas, deverá ser definida uma calendarização que tenha em conta as ameaças efetivas e minimize o impacto financeiro sobre os operadores.

5. Perspetiva da ENISA

O Projeto de Regulamento é em geral demasiado intrusivo também à luz do entendimento preconizado pela ENISA; deveria, por princípio, **impor objetivos deixando aos operadores maior liberdade de execução.** A ENISA propõe esta abordagem e sugere inclusive que o operador siga as boas práticas do mercado em termos de normas, nomeadamente a ISO 27001 ou a ISO 22301, com as quais até faz um mapeamento. Mais, conforme demonstrado nos comentários específicos, é possível a existência de uma abordagem alternativa assente nos objetivos de segurança propostos pela ENISA. Neste cenário seria possível permitir aos operadores reutilizar processos ou metodologias já adotadas, a fim de simplificar a implementação deste regulamento e não impor custos desproporcionais.

As normas técnicas sobre medidas de segurança da ENISA, sendo meras *guidelines*, não são vinculativas e referem explicitamente que cabe às ARN decidirem se impõem todas as medidas recomendadas, apenas parte, ou outras medidas. Contudo, a ANACOM adotou como medidas vinculativas, nalguns casos, **o nível 3 de sofisticação das medidas – *"State of the Art"*** propostas pela ENISA, que é o mais avançado e exigente, não sendo clara a justificação para esta opção no contexto nacional. Seria mais razoável definir o nível de sofisticação que se pretende para o

APRITEL – Associação dos Operadores de Comunicações Eletrónicas
Largo Rafael Bordalo Pinheiro, n.º 16 (ao Chiado) – Escritório 1.03, 1200-369 Lisboa
. Tel.: +351 213 550 911 • apritel@apritel.org • www.apritel.org • NIPC: 504 169 998

sector face à realidade do contexto atual e adotar uma **aproximação faseada, começando no nível 1 – "Básico".**

A orientação da ENISA foi a de cingir as medidas técnicas de execução aos incidentes que impliquem a interrupção da prestação dos serviços de comunicações eletrónicas, o que nem sempre é claro ao longo do Projeto de Regulamento, o que deverá ser clarificado, conforme já solicitado no ponto 1.3, alusivo ao *âmbito* do Projeto de Regulamento.

II - COMENTÁRIOS ESPECÍFICOS:

1. **Abordagem alternativa: fixação de objetivos de segurança**

A ANACOM pretende impor as medidas e processos (meios) a adotar quando, no entender da APRITEL, o foco deverá ser **o objetivo (fins) que se pretende atingir**, conforme define a ENISA nas *guidelines* abordadas no ponto anterior.

Com efeito, a APRITEL entende que na definição das medidas técnicas de execução deveriam ser estipulados objetivos a serem cumpridos por todos os operadores. Neste caso, a adoção de medidas concretas (ou seja, a metodologia usada) devem ser deixadas ao critério de cada operador dado que atualmente a maior parte dos operadores já as tem em vigor. Aliás, o próprio mercado e as condições específicas do setor das comunicações eletrónicas assim o exigem.

Esta abordagem foi prosseguida por reguladores de referência como a OFCOM e a COMREG, que optaram pela publicação de linhas de orientação sobre as obrigações em matéria de segurança e integridade de redes, nas quais definem um conjunto de objetivos a serem alcançados pelos operadores, garantindo porém alguma flexibilidade na definição das medidas a serem adotadas para alcançar estes fins. Em ambos os casos, quer seja na adoção dos requisitos mínimos de segurança pelos operadores, quer seja na própria aferição do seu cumprimento, estes reguladores recomendam que seja tido na máxima consideração a *Technical Guideline for Security Measures* da ENISA ("*linhas de orientação*").

A APRITEL considera que semelhante abordagem resulta em claros benefícios ao permitir que as medidas técnicas de execução sejam adaptadas à realidade de cada operador tendo por base objetivos definidos, evitando-se a imposição de soluções *one size fits all* que poderão revelar-se contraproducentes, desajustadas ou mesmo inexequíveis.

APRITEL – Associação dos Operadores de Comunicações Eletrónicas
Largo Rafael Bordalo Pinheiro, n.º 16 (ao Chiado) – Escritório 1.03, 1200-369 Lisboa
. Tel.: +351 213 550 911 • apritel@apritel.org • www.apritel.org • NIPC: 504 169 998

Conforme demonstrado no anexo I é possível efetuar uma correspondência quase integral entre os artigos apresentados no Projeto de Regulamento com os domínios e *objetivos de segurança* ('SO') apresentados pela ENISA nas suas linhas de orientação.

Neste sentido, a APRITEL toma a liberdade de sugerir a título ilustrativo dois exemplos de como se poderiam formular as regras num modelo de fixação de objetivos ('SO'), apresentando uma redação alternativa para dois artigos (12.º e 13.º)[1] assentes nos correspondentes SO, e onde:

a) Controlos: indicam as medidas organizacionais, processuais ou técnicas que devem ser garantidas de forma a atingir o objetivo de segurança, sendo que os operadores teriam a flexibilidade na adoção dos procedimentos mais ajustados para assegurar o cumprimento dos objetivos

b) Evidências: correspondem aos elementos a serem considerados como comprovativos na avaliação da execução e cumprimento destas medidas

Artigo 12.º Procedimento de Gestão de Alterações

Objetivo de Segurança: As empresas devem estabelecer Procedimentos de Gestão de Alterações a fim de minimizar a probabilidade de ocorrência de incidente de segurança que possa resultar dessas alterações.

Controlos	***Evidências***
• *Devem ser seguidos procedimentos operacionais predefinidos previamente à realização de alterações a sistemas críticos (SO 14)* • *Devem ser realizados testes de integração e de sistema previamente à introdução de alterações a sistemas críticos (SO 23)*	• *Documentação com descrição do procedimento operacional para execução de alterações (SO 14)* • *Relatório da realização dos testes (SO 23)*

i. Artigo 13.º - Sistemas de Controlo de Acessos

Objetivo de Segurança: As empresas devem estabelecer procedimentos de controlo de acessos físicos e lógicos que tenham em especial consideração os ativos constantes do Inventário de Ativos.

Controlo	***Evidência***

[1] Detalhes adicionais no anexo I

APRITEL – Associação dos Operadores de Comunicações Eletrónicas
Largo Rafael Bordalo Pinheiro, n.º 16 (ao Chiado) – Escritório 1.03, 1200-369 Lisboa
. Tel.: +351 213 550 911 • apritel@apritel.org • www.apritel.org • NIPC: 504 169 998

• *Devem ser implementados procedimentos que detetem ou evitem acessos físicos não autorizados a instalações* • *Devem ser implementados procedimentos de controlo de acesso lógico a ativos que permitam apenas uso autorizado* • *Deve ser avaliada periodicamente a eficácia dos procedimentos de controlo de acesso físico e lógico e realizadas melhorias, se necessário*	• *Demonstração da implementação de medidas de segurança física* • *Demonstração da implementação de medidas de autenticação e de controlo de acesso dos utilizadores aos ativos* • *Relatório da avaliação da eficácia das medidas de controlo de acesso físico e lógico*

Sugere-se que seja inicialmente escolhido o grau de sofisticação 1 proposto pela ENISA.

Salienta-se que semelhante exercício exemplificativo poderia ser transposto para a totalidade dos artigos apresentados no documento[2] em consulta, o que não prejudica o exercício de comparabilidade entre operadores, conforme refere a própria ENISA[3], acautelando assim uma preocupação da ANACOM.

Por entender que um regime que confira aos operadores flexibilidade na adoção de medidas técnicas de execução apresenta benefícios significativos, a APRITEL manifesta a sua total disponibilidade para integrar um grupo de trabalho em que seja avaliada uma abordagem alternativa, assente na definição de objetivos de segurança.

Sem prejuízo deste entendimento e disponibilidade, admitindo a possibilidade de a ANACOM manter a abordagem proposta no Projeto de Regulamento de segurança, apresentam-se de seguida os comentários específicos da APRITEL às obrigações e medidas vertidas no projeto de regulamento de segurança, sendo que os mesmos são igualmente relevantes numa perspetiva de definição do Regulamento numa lógica de objetivos de segurança, conforme proposto pela APRITEL.

2. Aspetos específicos da abordagem do Projeto de Regulamento

Os comentários da APRITEL à abordagem da ANACOM No Projeto de Regulamento versam as seguintes matérias em consulta:

- Classificação e inventário de ativos
- Gestão de riscos
- Dossier de segurança
- Exercícios de segurança e testes de resiliência
- Auditorias

[2] Exceção ao artigo 11.º associado à neutralidade de rede

[3] Enisa, *Technical Guideline for Minimum Security Measures,* Capítulos 5.2 a 5.4, pp. 28-33

APRITEL – Associação dos Operadores de Comunicações Eletrónicas
Largo Rafael Bordalo Pinheiro, n.º 16 (ao Chiado) – Escritório 1.03, 1200-369 Lisboa
. Tel.: +351 213 550 911 • apritel@apritel.org • www.apritel.org • NIPC: 504 169 998

Classificação e inventário de ativos:

i) Complexidade da classificação: considera-se que as regras relativas ao inventário de ativos impõem uma elevada complexidade, desde logo porque se prevê um número elevado de critérios e de complexa natureza. Esta complexidade e a excessiva dimensão do universo de ativos a inventariar tem depois repercussões nos processos subsequentes - gestão do inventário, análises de risco, etc.

ii) Onerosidade da gestão de um sistema tão complexo de inventariação: a manutenção e atualização dos vários atributos a constar para cada elemento do inventário de ativos exigem um esforço desmesurado. Com efeito, em resultado da classificação e inventariação propostas, estima-se a inclusão de um substancial_número de ativos por operador, o que implicará um elevado esforço para dar cumprimento aos processos decorrentes de qualquer alteração aos ativos (análises de riscos, gestão de alterações, etc.), particularmente com a frequência e prazos prescritos pela ANACOM.

iii) Riscos sobre a confidencialidade da informação: a partilha de informação sobre ativos, ainda que reduzida, acarreta riscos de fuga de informação.

Neste sentido, sugere-se uma simplificação, optando-se por uma classificação binária (apenas dois tipos de ativos) que tenha em conta a criticidade dos ativos, e que se divida em *ativos críticos* e *ativos não críticos*.

A comunicação da síntese do inventário de ativos, que inclui a respetiva localização geográfica, é contraproducente e acarreta riscos de fuga inadvertida de informação, situação que implica riscos sobre a confidencialidade dos ativos (artigos 7.º e 8.º do Projeto de Regulamento), sugerindo-se a sua eliminação. Contudo, tal não limita a possibilidade de acesso aos dados pela ANACOM através de consulta e de auditoria nas instalações do operador por técnicos credenciados e autorizados para o efeito.

Gestão de riscos:

O esforço e complexidade associados a uma ”Análise de Risco” global são extremamente elevados e não justificados no contexto nacional. Esta obrigação deve ser devidamente delimitada no seu âmbito e periodicidade.

A APRITEL sugere a eliminação desta obrigação genérica e a sua substituição pelo seguinte modelo:

APRITEL – Associação dos Operadores de Comunicações Eletrónicas
Largo Rafael Bordalo Pinheiro, n.º 16 (ao Chiado) – Escritório 1.03, 1200-369 Lisboa
. Tel.: +351 213 550 911 • apritel@apritel.org • www.apritel.org • NIPC: 504 169 998

- Uma *Análise de Risco Global* em que cada operador deverá ter processos internos definidos e apropriados para o fim a que concorrem e que essa mesma análise global não abranja a totalidade dos ativos, mas apenas um conjunto de ativos de maior criticidade. Propõe-se, ainda, que a periodicidade de revisão seja de dois em dois anos.

- Uma *Análise de Risco Específica* mediante notificação pela ANACOM da existência de um risco ou de uma ameaça que impliquem uma elevada probabilidade de ocorrência de violação de segurança ou perda de integridade com impacto significativo. Neste caso, a ANACOM poderá indicar medidas específicas de avaliação e esta análise deverá ser restrita aos ativos que possam ser impactados pela referida ameaça ou risco (Análise de Risco Parcial).

O prazo para a realização das análises de riscos (globais e parciais) deve ser suficiente para implementar os requisitos e as medidas técnicas e organizacionais que venham a ser definidos em resultado da análise, considerando a APRITEL que este prazo não deve ser inferior a 1 ano. A identificação das ameaças, internas ou externas, intencionais ou não intencionais, deve ainda estar limitada às causas efetivamente relevantes para identificação das ameaças em análise.

Dossier de segurança:

Especificamente sobre o dossier de segurança, a APRITEL propõe que se adote um princípio de desmaterialização e de minimização dos custos, de acordo com as melhores práticas.

Deve ser clarificado que a assinatura do dossier de segurança poderá efetuar-se através de assinatura digital, dispensando assim a manutenção em suporte físico do referido dossier, o que seria altamente ineficiente e contrário aos princípios de respeito pelo ambiente, bem como, a natureza das próprias comunicações eletrónicas e evolução tecnológica que se quer, cada vez mais, desmaterializada/digital.

Uma vez que a obrigação de manutenção das versões históricas, durante 5 anos, da documentação incluída no dossier, incluindo as cópias das notificações de segurança efetuadas, carece de fundamentação e razoabilidade, sugere-se a sua eliminação.

Exercícios de segurança e testes de resiliência:

A realização anual de exercícios de segurança e de testes semestrais aos diversos sistemas é excessiva e tem um impacto muito disruptivo na operação normal das

APRITEL – Associação dos Operadores de Comunicações Eletrónicas
Largo Rafael Bordalo Pinheiro, n.º 16 (ao Chiado) – Escritório 1.03, 1200-369 Lisboa
. Tel.: +351 213 550 911 • apritel@apritel.org • www.apritel.org • NIPC: 504 169 998

redes e serviços, dispondo já os operadores de processos cuja implementação visa o controlo da qualidade/continuidade da prestação dos serviços e tendo sempre em vista minimizar o impacto no Cliente. Ainda assim, existem situações em que não se consegue reduzir ou evitar completamente a disrupção do serviço prestado ao Cliente, pelo que deve ser deixado ao critério do operador quais os testes a realizar, quando e com que periodicidade.

Em alternativa aos testes semestrais, a APRITEL sugere a definição de um plano de exercícios com uma periodicidade razoável (exercícios anuais), com âmbito limitado em número de ativos abrangidos, mas em que seja assegurada a cobertura de ativos e sistemas relevantes no espaço de 5 anos. Por princípio, considera-se que devem ser os operadores a desenhar o seu **modelo** (desenho) de testes e a definir a respetiva **periodicidade** (testar sistemas ou testar as medidas). Deve caber à ANACOM a dinamização e coordenação dos exercícios que possam envolver diferentes intervenientes (intra e extra setor das comunicações eletrónicas).

Auditorias:

No Projeto de Regulamento estão ainda previstas auditorias que permitem aferir se os objetivos estabelecidos foram atingidos. No entanto, sendo os próprios operadores os principais interessados em manter a integridade e continuidade da prestação dos seus serviços, já dispõem de processos e medidas adequadas para as garantir.

Neste contexto, as auditorias devem ser feitas de acordo com um ciclo de melhoria contínua e tendo em conta a razoabilidade dos investimentos necessários para resolver as não conformidades.

A resolução de *'não conformidades'* deve ser focada nos objetivos a alcançar e não na forma concreta de alcançar estes objetivos, conforme a APRITEL tem vindo a afirmar ao longo do documento.

Tendo estes aspetos em consideração, sugere-se que seja eliminada do ponto 3 do art.º 36.º o seguinte texto relativo à resolução de não conformidades:

"*…e que todas são executadas dentro do prazo máximo que a ANACOM, caso assim o entenda, venha a determinar.*"

No período inicial de implementação do Regulamento, com vista à minimização de custos, sugere-se recorrer a Auditores internos, devidamente qualificados e certificados por normativos usados no setor.

APRITEL – Associação dos Operadores de Comunicações Eletrónicas
Largo Rafael Bordalo Pinheiro, n.º 16 (ao Chiado) – Escritório 1.03, 1200-369 Lisboa
. Tel.: +351 213 550 911 • apritel@apritel.org • www.apritel.org • NIPC: 504 169 998

No âmbito do dever de colaboração, qualquer contacto com os fornecedores relevantes ao nível da segurança e integridade das redes e serviços deve ser efetuado pelos e/ou com conhecimento e participação dos operadores de comunicações eletrónicas.

CONCLUSÕES

Em resumo, pode sintetizar-se o teor das preocupações fundamentais da APRITEL nos seguintes pontos:

I. O Projeto de Regulamento não se encontra adequadamente fundamentado, em particular no que respeita à proporcionalidade e razoabilidade das obrigações impostas;

II. As medidas de execução impostas são demasiado intrusivas e excessivas face à realidade nacional, não se reconhecendo razões para que Portugal adote um regime bastante mais exigente do que o que existe na generalidade dos restantes países;

III. A ANACOM deveria privilegiar um regime assente no sentido de responsabilidade dos operadores para implementação das medidas técnicas e organizacionais adequadas à garantia da segurança das suas redes e dos seus serviços tendo em consideração os riscos existentes;

IV. Para o efeito apresenta-se, através da formulação de exemplos ilustrativos, uma possível abordagem alternativa assente nos objetivos de segurança e respetivos controlos definidos pela ENISA nas suas linhas de orientação;

V. O envio periódico de informação crítica à ANACOM constitui, por si só, um risco de segurança que deve ser evitado;

VI. Os exercícios de segurança e os testes aos diversos sistemas de controlo devem ser faseados em número de ativos e com uma periodicidade superior a 6 meses;

VII. As auditorias devem ser integradas num ciclo de melhoria contínua com atenção à razoabilidade dos investimentos necessários.

APRITEL – Associação dos Operadores de Comunicações Eletrónicas
Largo Rafael Bordalo Pinheiro, n.º 16 (ao Chiado) – Escritório 1.03, 1200-369 Lisboa
. Tel.: +351 213 550 911 • apritel@apritel.org • www.apritel.org • NIPC: 504 169 998

É com a maior expetativa que a APRITEL apela ao acolhimento das sugestões aqui apresentadas.

Junta um anexo **Mapeamento entre os artigos do projeto de regulamento e SO apresentados pela ENISA nas Technical Guideline on Security Measures**

APRITEL – Associação dos Operadores de Comunicações Eletrónicas
Largo Rafael Bordalo Pinheiro, n.º 16 (ao Chiado) – Escritório 1.03, 1200-369 Lisboa
. Tel.: +351 213 550 911 • apritel@apritel.org • www.apritel.org • NIPC: 504 169 998

Anexo I

A: Mapeamento entre os artigos do projeto de regulamento e SO apresentados pela ENISA nas Technical Guideline on Security Measures[1].

Tabela 1: Relação entre artigos do projeto de regulamento e os objetivos de segurança[2]

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

[1] ENISA, versão 2.0, October 2014

[2] Foram considerados os artigos do projeto de regulamento associados às obrigações/ medidas (artigos 7.º a 36.º)

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