[redacted]

From: [redacted]@telecom.pt>
Sent: 14 de março de 2017 17:27
To: regulamento.seguranca@anacom.pt
Subject: MEO - Pronúncia sobre o projeto de regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas
Attachments: 20170314_proj-reg-segurança_meo.pdf; 20170314_proj-reg-segurança_meo_vnc.pdf; 20170209_anexo_security and integrity obligations_benchmark.xlsx

Exmos Srs.

Na sequência da carta com a refª S0120, remetida nesta data sobre o assunto em epígrafe e conforme solicitado pela ANACOM, enviamos junto a pronúncia da MEO sobre o projeto de regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas, acompanhada de uma versão expurgada dos elementos considerados confidenciais e do anexo (ficheiro Excel) com a análise de *benchmark* realizada pela MEO.

Com os melhores cumprimentos,

PT

[redacted]

PRONÚNCIA DA

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

AO

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

VERSÃO NÃO CONFIDENCIAL

14.03.2017

ÍNDICE

NOTA PRÉVIA

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

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

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

I. COMENTÁRIOS GERAIS

1. A segurança e integridade das redes de comunicações eletrónicas e a continuidade dos serviços nestas suportados são preocupações primárias dos prestadores de redes e serviços de comunicações eletrónicas, dada a relevância destas matérias para determinados fatores críticos de sucesso do seu negócio, como sejam a proteção (segurança em sentido estrito) dos seus ativos, a qualidade dos serviços prestados, a confiança e satisfação dos clientes ou a reputação das empresas no mercado.

2. Para além desta motivação económica, endógena, para zelar pela segurança e integridade das redes e serviços de comunicações eletrónicas, as respetivas empresas prestadoras estão obrigadas, nos termos do Artigo 54.º-A da Lei das Comunicações Eletrónicas (doravante "LCE"), a *adotar as medidas técnicas e organizacionais adequadas à prevenção, gestão e redução dos riscos para a segurança* [e integridade] *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*, devendo tais medidas ser *adequadas aos riscos existentes tendo em conta o estado da técnica*.

3. Enquanto operador de referência e de grande relevo em Portugal, nomeadamente pelo seu papel histórico no sector, a MEO sempre primou pela segurança e integridade das suas redes e serviços. Estes aspetos sempre foram centrais na estratégia da empresa para cumprir com as diversas responsabilidades que lhe foram cometidas e para se diferenciar no mercado face aos seus concorrentes pelo que, ao longo da sua história, a MEO procedeu a diversas adaptações e transformações, quer do ponto de vista tecnológico, quer do ponto de vista organizativo, instituindo um processo de melhoria contínua da sua capacidade de avaliação de riscos e de gestão da segurança e integridade das redes e serviços, tendo em consideração as melhores práticas e as normas internacionais relevantes.

4. Consequentemente, a MEO está a cumprir as obrigações determinadas na LCE sobre esta matéria, suportando-se para tanto na sua própria experiência e em processos, tecnologias e sistemas que evoluíram (e continuam a evoluir) ao longo do tempo, otimizando continuamente o nível de eficiência das medidas adotadas tendo em conta a evolução tecnológica, os riscos existentes e as especificidades da organização.

5. Neste enquadramento, e sem prejuízo de se reconhecer que podem existir objetivos de segurança a nível nacional que extravasam os interesses próprios dos operadores, o Projeto de Regulamento colocado em consulta pública pela ANACOM surpreende negativamente por duas ordens de razão principais: por um lado, determinados artigos assumem um carácter prescritivo e focado na forma como os operadores devem cumprir as suas obrigações relativamente à segurança e integridade das suas redes e serviços quando, no entender da MEO, o foco principal deverá ser colocado nos fins (objetivos de segurança) que se pretendem atingir.

6. Por outro lado, o Projeto de Regulamento surge alheado de uma análise à forma como os operadores dão cumprimento às suas obrigações nesta matéria, de uma demonstração da necessidade de impor medidas adicionais e com tal grau de especificação, e da ponderação cuidada da eficácia e dos méritos incrementais destas medidas face aos custos de conformação que acarretam para os operadores (que o Projeto de Regulamento subestima de forma significativa), resultando numa proposta, no seu todo, desproporcional.

7. Considerando as competências e os deveres que lhe estão atribuídos na LCE, a ausência de medidas técnicas de execução da Comissão Europeia previstas no n.º 4 do Artigo 13.º-A da Diretiva-Quadro (para harmonizar a gestão da segurança e integridade das redes e serviços ao nível da União) e a amplitude das linhas de orientação publicadas pela Agência Europeia para a Segurança das Redes e da Informação (ENISA), a ANACOM goza de uma assinalável liberdade de atuação para decidir se e que medidas deve impor aos operadores neste campo, circunstância que também lhe impõe, em contrapartida, especiais responsabilidades na escolha e justificação dessas decisões, nomeadamente à luz do contexto nacional.

8. Neste sentido, a MEO considera que vários aspetos do Projeto de Regulamento devem ser consideravelmente revistos ou mesmo eliminados, conforme comentários detalhados no capítulo seguinte, com o objetivo de tornar proporcional e adequado à realidade nacional o quadro das obrigações a fixar nesta matéria, repousando mais na independência e sentido de responsabilidade dos operadores para implementarem as medidas técnicas e organizacionais adequadas à prossecução dos objetivos de segurança e integridade nas suas redes e serviços, sem prejuízo da supervisão e controlo do cumprimento destes objetivos por parte do Regulador.

9. A orientação genérica que a MEO defende neste assunto encontra respaldo no documento da ENISA de outubro de 2014 "*Technical Guideline on Security Measures - Technical guidance on the security measures in Article 13a*" que, no entender da MEO, é uma referência chave para este processo.

10. Sendo certo que estas linhas de orientação da ENISA não são vinculativas e que a abordagem proposta pela ANACOM no Projeto de Regulamento também ali encontra enquadramento, o que importa realçar, no entender da MEO, é a forma como a ENISA reconhece a heterogeneidade que caracteriza o sector das comunicações eletrónicas, com operadores associados a diversos portfólios de serviços, tecnologias e graus de maturidade (alertando que *one size does not fit all*), e prevê a possibilidade das ARN usarem as linhas de orientação de forma diversa, menos prescritiva, mais enquanto *recomendação* e instrumento de supervisão.

11. A este respeito, sublinha-se que o documento da ENISA refere logo no Prefácio (pág. 3) que "*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.*", orientação fundamental que a MEO entende dever ser mantida e estar presente em todo este processo para evitar excessos na imposição de obrigações aos operadores relacionadas com a segurança e integridade das suas redes e serviços.

12. Tendo em conta as linhas de orientação constantes nos pontos 4 e 5 do referido documento da ENISA, a MEO sugere que se adote a seguinte abordagem genérica:

    (i) Estabelecer a correspondência entre os artigos/medidas técnicas de execução apresentados no Projeto de Regulamento de segurança e os domínios e objetivos de segurança (SO) apresentados pela ENISA no referido documento.

    Ver o ponto 5.1.2 – *Using the ENISA guideline as a recommendation*, bem como a resposta da APRITEL a esta consulta pública, a qual inclui um mapeamento possível entre os artigos do Projeto de Regulamento com os domínios e objetivos de segurança (SO) da ENISA.

    (ii) Determinar a autoavaliação dos prestadores de redes e serviços de comunicações eletrónicas quanto à implementação das medidas/objetivos de segurança identificados no ponto anterior, obtendo assim uma visão geral do *nível de sofisticação* de cada prestador e do sector em geral na escala proposta pela ENISA (*1 – Basic, 2 – Industry standard, 3 – State of the art*).

    (iii) Identificar, a partir da análise anterior, quais os objetivos e respetivas medidas de segurança relevantes que requerem atenção específica no contexto nacional.

(iv) Definir uma estratégia por etapas para cumprimento dos objetivos definidos ou para elevação do nível de sofisticação das medidas adotadas pelos prestadores, conferindo-lhes tempo e flexibilidade para se adaptarem.

Ver o ponto *5.3 – Taking a staged approach* para mais detalhes.

(v) Não decidir pela imposição de medidas de segurança específicas que limitam a flexibilidade dos operadores para cumprirem o(s) objetivo(s) de segurança subjacente(s), sem que haja razões de peso que o justifiquem (incidentes de larga escala ou demasiado frequentes, por exemplo) e sem que antes a eficácia e razoabilidade dessas medidas tenha sido aferida junto dos operadores.

Ver ponto *5.1.1 – Mandating versus recommending a security standard* para mais detalhes.

(vi) Determinar aos prestadores de redes e serviços de comunicações eletrónicas a realização de auditorias, conforme previsto no Artigo 54.º-F da LCE, nos termos necessários ao acompanhamento e supervisão do cumprimento dos objetivos e medidas de segurança.

13. A MEO está convencida que, ao contrário do que resulta do Projeto de Regulamento, a definição das obrigações em matéria de segurança e integridade de redes e serviços de comunicações eletrónicas segundo as linhas enunciadas no ponto anterior permitirá tirar partido dos processos e das medidas já instituídas pelos operadores e garantir que as eventuais novas obrigações a fixar sejam realmente necessárias e proporcionais.

14. No capítulo seguinte, a MEO apresenta os comentários específicos que as diversas partes do Projeto de Regulamento lhe suscitam.

II. COMENTÁRIOS ESPECÍFICOS

Nota Justificativa

15. Antecipa-se a partir dos comentários anteriores que a MEO considera que a Nota Justificativa constante do Projeto de Regulamento não se encontra devidamente fundamentada, em particular no que respeita à necessidade e proporcionalidade das obrigações que o Projeto de Regulamento pretende impor.

16. Efetivamente, a Nota Justificativa limita-se a declarar que "*Na regulamentação das obrigações das empresas em matéria de segurança e integridade das redes e serviços, foram objeto de ponderação, por um lado, os custos a incorrer pelas empresas no cumprimento das suas obrigações e, por outro, os benefícios daí emergentes, os quais incluem* (…)" e não apresenta qualquer elemento adicional que sustente tal ponderação, o que se afigura manifestamente insuficiente.

17. A este respeito, a MEO considera que o Projeto de Regulamento constitui um exemplo paradigmático da necessidade da ANACOM incorporar no seu processo regulatório uma prática sistemática e estruturada de Avaliação de Impacto Regulatório (AIR), conforme esta empresa já defendeu em diversas ocasiões.

18. Se um processo de AIR estivesse instituído, a Nota Justificativa não seria omissa em relação a etapas fundamentais do processo regulatório como, desde logo, a caracterização do problema que se pretende resolver, a definição dos objetivos a atingir, a identificação das várias alternativas de atuação e a avaliação dos custos e méritos de cada alternativa que permitisse justificar a opção final escolhida.

19. De qualquer forma, mesmo não tendo um sistema estruturado de AIR incorporado no seu processo regulatório, faz-se notar que a ANACOM está obrigada a pautar a sua atuação pela observância do princípio da proporcionalidade, que é um princípio basilar do ordenamento jurídico comunitário. Segundo a própria ANACOM[1], citando A. MATTERA: "*Uma dada medida só poderá ser considerada aceitável em face do direito comunitário se por um lado existir um adequado nexo de causalidade entre essa medida e o objetivo legítimo prosseguido, se por outro lado, os meios adotados para atingir tal objetivo deverem ser considerados necessários – isto é, suficientes e não excessivos; e, finalmente, se não houver outras medidas menos severas que, bastando para atingir eficazmente o objetivo visado, comportem menos perturbações do tráfico jurídico-mercantil e sejam, por isso, menos opressivas para os operadores económicos do mercado comum.*"

20. Porém, como já se disse, nem a Nota Justificativa, nem o Projeto de Regulamento no seu todo, contêm elementos que permitam afirmar que a ANACOM tomou o princípio da proporcionalidade em devida consideração na análise que efetuou, nem sequer através de uma análise de

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

benchmark com outros países, recurso que é relativamente comum utilizar-se, nomeadamente quando a avaliação direta da proporcionalidade é difícil de realizar — o que não se concede que seja o caso presente.

21. A falta de fundamentação do Projeto de Regulamento é uma falha especialmente grave face ao nível de interferência na organização e vida interna das Empresas e ao grau de exigência que está subjacente às medidas propostas.

22. Enquanto contributo para uma nova reflexão sobre esta matéria, a MEO remete em Anexo[2] a esta pronúncia a análise de *benchmark* que realizou a partir dos elementos que obteve via *Cullen International* relativos à implementação de medidas de segurança e integridade de redes em Espanha, França, Itália, Bélgica, Irlanda e Suécia. As principais conclusões desta análise são:

(i) As propostas avançadas pela ANACOM no Projeto de Regulamento consubstanciam o regime mais exigente de entre este grupo de países;

(ii) O regime sueco é o que mais se aproxima, mas com prazos de implementação mais dilatados e menos exigências de reporte. Nos restantes países as medidas específicas não têm o detalhe e a abrangência do Projeto de Regulamento da ANACOM;

(iii) Em geral, estes regimes impõem obrigações genéricas de garantir a segurança e integridade das redes e das infraestruturas críticas e assentam no sentido de responsabilidade dos operadores para implementarem as medidas adequadas para cumprimento daquelas obrigações.

Cita-se, a título de exemplo, a seguinte passagem da decisão da ComReg sobre esta matéria: "*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.*"

23. **[IIC]** [redacted]

[2] Ficheiro "20170209_anexo_security and integrity obligations_benchmark.xlsx".

[redacted] **[FIC]**

24. A MEO desconhece e duvida da existência de circunstâncias específicas nacionais, seja do ponto de vista geopolítico, geológico, climatérico ou histórico que possam justificar a implementação em Portugal de medidas de segurança e integridade de redes e serviços de comunicações eletrónicas com um nível de exigência superior ao dos restantes países, e com custos de implementação tão significativos que não deixariam de impactar na economia das empresas e, a final, o próprio mercado.

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

Título I – Disposições gerais

Artigo 2.º - Âmbito

26. A MEO não entende o alcance da referência aos equipamentos localizados nas instalações do Cliente que é efetuada no n.º 3 do Artigo 2.º e sugere a sua eliminação. É de notar que mesmo que a gestão destes equipamentos seja feita pela MEO, não é possível assegurar a este nível o mesmo grau de segurança e integridade que se exige relativamente aos ativos na rede do operador. Em primeiro lugar, existem Clientes (empresariais) que exigem, pese embora a gestão estar confiada à MEO, ter acesso aos equipamentos localizados nas suas instalações. Em segundo lugar, porque estando os equipamentos localizados em instalações do Cliente, o operador não pode garantir que estes não sejam acedidos indevidamente, seja através de ligações físicas, seja através das redes internas do Cliente cujas políticas de segurança o operador não controla.

Artigo 3.º - Definições

27. Não é totalmente evidente a que se refere a palavra “infraestruturas” na alínea c) do n.º 1 (definição de Ativos). Trata-se de infraestruturas civis, como edifícios? Solicita-se que esta questão seja clarificada.

28. Também não é evidente o significado de “centro principal de gestão e operação” pelo que se solicita a definição deste conceito.

29. A definição de "Incidente de segurança" constante na alínea g) do n.º 1 é mais complexa que a definição utilizada pela ENISA (*Security incident: A breach of security or a loss of integrity that could have an impact on the operation of electronic telecommunications networks and services*). A ANACOM adiciona à definição o conceito de *evento com impacte negativo real no funcionamento ou na segurança ou integridade das redes e serviços* mas não se percebe qual a utilidade do complemento. Sugere-se, por isso, que a definição seja revista de modo a ficar em linha com a definição da ENISA.

30. Ainda a este propósito recorde-se a posição anteriormente assumida pela ANACOM sobre este ponto, nomeadamente no Relatório da Audiência Prévia e do procedimento geral de consulta sobre o sentido provável de decisão relativo a violações de segurança e perdas de integridade nas redes e serviços de comunicações eletrónicas, aprovado por Deliberação Conselho de Administração de 12 de dezembro de 2013, através do qual o Regulador entendeu que não era importante a definição de um conceito de "incidente de segurança" por não corresponder "(…) *a um conceito preciso e fechado* (…)" (pág. 2).

31. A própria ANACOM admitiu que se tratava de um conceito que ao nível do quadro comunitário e nacional não se encontrava definido e que o principal motivo prendia-se com o facto de o relevante ser as Autoridades Reguladoras conhecerem efetivamente as causas que originavam as perturbações no funcionamento dos serviços prestados pelas redes e serviços de comunicações eletrónicas.

32. Naquela ocasião a ANACOM indicou, ainda, que o importante não era a definição do conceito, mas sim o resultado, ou seja, o que importava era a notificação de determinado evento e não tanto o enquadramento.

33. Por outro lado, a definição de "Integridade" está omissa deste artigo, o que dificulta a compreensão do conceito. A MEO sugere a inclusão da definição de "Integridade" na versão final do Projeto de Regulamento, tomando por base a definição considerada pela ENISA (*In technical literature about networks and network inter-connections, the term integrity is defined as "the ability of the system to retain its specified attributes in terms of performance and functionality"*).

34. A MEO não compreende o alcance do n.º 2 do Artigo 3.º e por que razão se refere apenas à Região Autónoma da Madeira.

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

Artigo 6.º - Medidas técnicas de execução e requisitos adicionais

35. Como decorre dos pontos anteriores deste documento, a MEO considera que não existem razões que justifiquem a imposição de medidas de segurança e integridade com o nível de especificação e a abrangência previstos no Artigo 6.º, bem como nos artigos subsequentes para os quais este remete.

36. Consequentemente, a MEO defende que este Artigo (e os subsequentes) sejam alterados em linha com a abordagem genérica que esta empresa preconiza, definindo-se as medidas técnicas de execução a impor ao abrigo do Artigo 54.º-C da LCE após uma avaliação prévia das medidas já implementadas pelas Empresas e do nível de cumprimento dos objetivos de segurança.

37. Na medida do possível e do que for considerado adequado, contando também com a avaliação pelas Empresas, as medidas a impor deverão ser centradas nos objetivos que se pretenderem assegurar (por oposição a determinarem formas concretas de alcançar esses objetivos) e prever o cumprimento das obrigações por etapas.

Artigo 7.º - Classificação de ativos

38. A MEO não reconhece qualquer vantagem em adotar uma classificação dos ativos em quatro categorias (de A a D), definidas através dos limiares especificados para a notificação das violações de segurança ou perdas de integridade.

39. Atendendo às restantes obrigações que o Projeto de Regulamento pretende impor associadas à classificação dos ativos (por exemplo, ao nível da gestão de riscos), é necessário que a classificação dos ativos e respetivas obrigações subsequentes não redunde em esforços desproporcionais. A este respeito, faz-se notar que a consideração dos ativos da Classe C (conforme proposta pela ANACOM, referentes a ativos dos quais dependam entre 10.000 e 100.000 acessos ou assinantes) implicaria esforços significativamente superiores e com ganhos meramente marginais ao nível da QoS assegurada face à consideração dos ativos das Classes A e B.[3]

[3] **[IIC]** [redacted] **[FIC]** A MEO considera que a inclusão da Classe C no Projeto de Regulamento é claramente desproporcional e excessiva.

40. A MEO considera, assim, esta classificação demasiado complexa e exigente pelo que defende a sua simplificação para um sistema binário, que classifique os ativos em críticos e não críticos, em função da percentagem de parque total de acessos ou assinantes do(s) serviço(s) abrangido(s) e da importância do ativo para o negócio.

41. Para além desta divergência de fundo, há ainda outros aspetos deste Artigo que suscitam as maiores reservas.

42. A MEO opõe-se à inclusão na Classe A e respetivas obrigações subsequentes dos ativos de que dependa a oferta de redes e serviços através dos quais seja assegurada a continuidade da prestação dos *serviços relevantes à sociedade e aos cidadãos*, por parte dos "Clientes relevantes" cuja identificação está prevista na al. f) do n.º 3 do Artigo 24.º que, por sua vez, remete para o n.º 6 do mesmo artigo 24.º. Esta disposição cria ambiguidade, dado o grau de discricionariedade da ANACOM na identificação dos "Clientes relevantes" e a incerteza quanto ao grau de dependência dos serviços ditos *relevantes* da oferta de redes e de serviços de comunicações eletrónicas.

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

44. Por outro lado, afigura-se particularmente iníquo que os operadores de redes e os prestadores de serviços de comunicações eletrónicas possam ficar sujeitos a obrigações adicionais específicas relacionadas com os "Clientes relevantes" quando, no sentido inverso, não beneficiam de igual tratamento preferencial (como é o caso com o fornecimento de energia elétrica, por exemplo).

45. Na identificação e classificação dos ativos críticos, chama-se ainda a atenção para as alíneas e) do n.º 3 e d) do n.º 5: é complexo, se não mesmo inviável do ponto de vista técnico, contabilizar o n.º de assinantes ou de acessos abrangidos na interligação entre redes, pelo que este critério deve ser eliminado.

46. A MEO também não concorda com o disposto no n.º 8 do Artigo 7.º, o qual prevê que a ANACOM, no âmbito do planeamento civil de emergência ou de um plano de emergência de proteção civil, possa identificar e impor às Empresas a identificação e classificação de determinados ativos. Com efeito, cabe às Empresas decidir quais os ativos essenciais ou críticos para assegurar o cumprimento dos objetivos e obrigações de segurança que lhes sejam fixadas no âmbito invocado pela ANACOM, sendo de todo improvável que a ANACOM possa estar em melhor posição para tomar, i.e., impor decisões a este nível de detalhe. As circunstâncias contratuais em que estes ativos estão abrangidos não poderão ser alteradas sem o prévio consentimento da MEO ou acordo entre todas as partes envolvidas.

Artigo 8.º - Inventário de Ativos

47. Para além do que decorre dos comentários anteriores relativamente à classificação dos ativos, a MEO considera excessivo o previsto no Artigo 8.º quanto ao inventário de ativos. Não se entende a necessidade de se entrar em tais níveis de detalhe relativamente à caracterização dos ativos, questão que deve caber às Empresas definir. A MEO sugere que os elementos definidos no ponto 2 deste Artigo constituam uma recomendação que as Empresas devam levar em linha de conta na elaboração e manutenção do seu inventário de ativos.

48. Adicionalmente, a MEO opõe-se a que a informação com este nível de detalhe e sensibilidade, mesmo que em formato de síntese, seja enviada à ANACOM, conforme previsto no n.º 4 deste Artigo. A transmissão deste tipo de informação é, em si mesma, uma vulnerabilidade de segurança que deve ser evitada. A MEO propõe que esta disposição seja alterada e passe a prever a obrigação das Empresas disponibilizarem esta documentação para consulta, nas suas instalações, a interlocutores da ANACOM devidamente credenciados e habilitados para o efeito.

Artigo 9.º - Gestão dos riscos

49. Este Artigo é dos que mais revelam o carácter prescritivo do Projeto de Regulamento e reflete uma preocupação (deslocada) quanto à *forma* como as empresas devem efetuar a gestão de riscos em vez de se centrar no objetivo de assegurar que as Empresas têm esse processo de segurança já implementado de forma adequada.

50. Não existe qualquer justificação para o esforço e a complexidade associados às medidas previstas neste Artigo, quer a nível da carga documental exigida, da abrangência da análise, da periodicidade ou dos fatores a considerar.

51. A MEO entende, por isso, que esta medida deve ser devidamente delimitada no seu âmbito e periodicidade, pelo que sugere uma abordagem alternativa, distinguindo Análises de Risco Globais de Análises de Risco Parciais.

52. No que se refere às Análises de Risco Globais, a obrigação deverá ser a de que cada operador implemente uma política interna de análise de riscos de acordo com os procedimentos que considere mais adequados, que abranja o conjunto de ativos de maior criticidade e com uma periodicidade não inferior a dois anos.

53. As Análises de Risco Parciais deverão ser estimuladas com a 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. Esta análise deverá cingir-se aos ativos que possam ser impactados pela referida ameaça ou risco. Admite-se que a ANACOM possa indicar, nestas situações, medidas específicas de avaliação da análise de risco.

Artigo 10.º - Medidas de Redundância, de Robustez e de Resiliência

54. Aplica-se a este Artigo o mesmo tipo de comentário efetuado ao Artigo 9.º. É intrusiva e deslocada a definição, pela ANACOM, de aspetos concretos da forma como as Empresas devem assegurar a redundância e resiliência das suas redes e serviços, como seja a autonomia dos ativos em caso de falha de abastecimento de energia ou a realização de testes semestrais às medidas adotadas. São questões intrinsecamente ligadas ao sucesso do negócio dos operadores e aos níveis de SLA a que estes se comprometem pelo que não carecem de tal especificação por parte da ANACOM.

55. Consequentemente, a MEO defende que este Artigo seja substancialmente aligeirado e reformulado em torno da obrigação genérica das Empresas deverem adotar as medidas de redundância, robustez e resiliência adequadas face aos ativos que possuem, às redes e serviços que operam e aos riscos e ameaças que enfrentam.

56. No que se refere aos testes, devem ser as Empresas a desenhar o seu modelo e a definir a respetiva periodicidade, tendo em vista a minimização dos impactos que estes testes podem ter no

funcionamento das redes e dos serviços, atendendo a que certo tipo de testes implica a interrupção da prestação do serviço.

Artigo 11.º - Procedimentos de Controlo da Gestão Excecional de Tráfego no Acesso à Internet

57. Tendo em conta que este Artigo diz respeito à gestão excecional de tráfego no acesso à internet, as referências no n.º 4 a) à *reserva de capacidade para comunicações de emergência de interesse público* e no n.º 4 b) à *priorização de tráfego nas situações extraordinárias previstas nas subalíneas iv) a vii) da alínea b) do n.º 1 do Artigo 2º* não permitem perceber que comunicações é que estão em causa, nem que tráfego deverá ser priorizado. Adicionalmente, não se afigura tecnicamente exequível o cumprimento destas obrigações indistintamente da especificidade das situações extraordinárias pelo que o descritivo genérico preconizado não é aceitável.

Artigo 12.º - Procedimentos de Gestão de Alterações

58. Em linha com a posição anteriormente assumida pela MEO, deve ser do critério e responsabilidade das Empresas a definição do âmbito, metodologia e as circunstâncias de aplicação dos procedimentos de Gestão de Alterações.

Artigo 14.º - Sistemas de Monitorização e Controlo

59. A MEO contesta a alínea b) do n.º 2 e o n.º 3 deste Artigo: não se considera uma mais valia exigir que os sistemas de monitorização e controlo sejam revistos anualmente e submetidos a testes semestralmente, dado que estes por definição são objeto de monitoria e controlo contínuo em regime de 24hx7 dias.

60. A MEO discorda também do n.º 4 deste Artigo pela elevada carga burocrática documental que implica, sem proveitos (técnicos, operacionais, QoS, etc.) ou com eventuais melhorias residuais e por conseguinte claramente desproporcionais.

Artigo 15.º - Exercícios

61. Compete às Empresas definir o âmbito e os objetivos do seu plano de exercícios de avaliação de segurança e integridade e salvaguardar que este não motive quaisquer impactos na normal operação das suas redes e serviços.

62. A MEO sugere a definição de um plano de exercícios com uma periodicidade que seja definida pelas Empresas em função do nível de risco dos seus ativos críticos.

63. Deve caber à ANACOM a dinamização e coordenação dos exercícios que possam envolver diferentes intervenientes dentro e fora do sector das comunicações eletrónicas.

Artigo 16.º - Prestação de informação aos clientes

64. Atenta à especificidade das entidades identificadas no n.º 6 do Artigo 24.º, a MEO não está autorizada a divulgar a terceiros (por obrigações contratuais) as circunstâncias em que ocorreram os incidentes, ameaças ou vulnerabilidades subjacentes ao Artigo 16.º dado que, nalguns casos por questões de Segurança Nacional, as respetivas entidades pretendem manter total reserva sobre estas matérias.

Artigo 17.º - Caracterização Geral da Segurança

65. A MEO considera que os elementos requeridos no n.º 1 deste Artigo tornam esta medida excessiva pela elevada carga burocrática documental que implica.

Artigo 18.º - Plano de Segurança

66. A MEO discorda do teor deste Artigo na sua globalidade pois o Plano de Segurança deve ser definido pelas Empresas de acordo com o âmbito das suas redes e serviços e os objetivos de segurança e níveis de resiliência estabelecidos internamente.

67. Solicita-se que seja esclarecido o que se entende por "comunicações de emergência de interesse publico" e por "situações de emergência" referidas nas alíneas b) e c) do ponto 3, do Artigo 18ª, respetivamente.

68. A MEO discorda do n.º 4 deste Artigo por considerar excessiva a revisão anual do Plano de Segurança. A MEO sugere que esta periodicidade passe a bienal.

Artigo 21.º - Ponto de Contacto Permanente

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

Artigo 22.º - Equipa de Resposta a Incidentes de Segurança

70. A redação deste Artigo não é totalmente clara ao referir que as *empresas devem assegurar <u>o acesso aos serviços de</u> Equipa de Resposta a Incidentes de Segurança* (…). A MEO entende que o sentido seja o de que *as empresas devem assegurar <u>a existência de uma</u> Equipa de Resposta a Incidentes de Segurança* (…), sugerindo-se esta revisão de redação à ANACOM.

Artigo 23.º - Dossier de Segurança

71. A MEO não reconhece especial vantagem em agregar toda a informação indicada neste Artigo num mesmo *dossier* e considera esta medida excessiva pela carga burocrática e documental que implica, pelo que defende a sua eliminação.

72. Caso se mantenha esta medida, a MEO defende que, pelo menos, deverá ser clarificado que os diversos documentos podem ser compilados em separado, dada a sensibilidade da sua informação, em formato eletrónico e assinados digitalmente.

73. Além disso, a obrigação de manutenção das versões históricas dos últimos 5 anos da documentação incluída no *dossier*, incluindo das cópias das notificações de segurança efetuadas, carece de fundamentação e razoabilidade, sugerindo-se a sua eliminação.

<u>Título III - Obrigações de notificação e de informação ao público</u>

Artigo 24.º - Circunstâncias

74. O n.º 2 deste Artigo deverá excluir do âmbito do impacto significativo as intervenções planeadas em horário noturno.

75. No que se refere à alínea f) do n.º 3, a MEO remete para o comentário efetuado acima relativamente ao Artigo 16.º. As obrigações de comunicar violações de segurança e perdas de integridade que envolvam entidades críticas para a segurança nacional como a Rede Nacional de Segurança Interna (doravante "RNSI") ou as restantes entidades identificadas, devem ser asseguradas diretamente por estas entidades.

76. De igual forma, as obrigações previstas na alínea b) do n.º 3 relativas ao 112 devem ser asseguradas pelo MAI, conforme posição já manifestada pela MEO em sede de resposta à consulta pública de dezembro de 2011.

77. No que respeita ao n.º 6 deste artigo, e em particular à alínea d), a MEO reitera os comentários já efetuados no âmbito do artigo 7.º quanto à iniquidade que resultará do facto dos operadores de comunicações eletrónicas passarem a estar sujeitos a obrigações adicionais específicas relacionadas com "Clientes relevantes".

Artigo 25.º - Formato e Procedimentos

78. A MEO, atendendo à sua experiência nesta matérias e aos tipos de incidente que se têm vindo a verificar desde a entrada em vigor da Deliberação de 12.12.2013, considera que no n.º 10 deste Artigo devem ser incluídas as causas raiz "Equipamento de Cliente" e "Intervenção Planeada".

79. Sugere-se ainda que a alínea a) do n.º 12 seja complementada com a obrigação da ANACOM informar as empresas com 10 dias úteis de antecedência sempre que forem alterados o endereço de correio eletrónico e/ou o número de telefone publicados no *site* institucional da ANACOM na Internet.

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

Artigo 27.º - Conteúdo, meios e prazos de divulgação

81. Na alínea c) do n.º 1 deste Artigo, considera-se que devem ser consideradas as horas úteis normais de funcionamento das empresas (i.e., das 09:00 às 17:00). Face à experiência dos três anos decorridos desde a decisão relativa a violações de segurança e perdas de integridade nas redes e serviços de comunicações eletrónicas, aprovada por Deliberação Conselho de Administração de 12 de dezembro de 2013, a MEO não vê razões para que se mantenha a exigência de um horário alargado (das 09:00 até às 19:00).

Título IV - Auditorias à segurança das redes e serviços

Artigo 35.º - Fase de Auditoria

82. Os colaboradores da ANACOM que assistam às Auditorias também devem obedecer às obrigações descritas no Artigo 31.º, nomeadamente no que diga respeito à credenciação adequada emitida por entidades competentes para acesso a matéria classificada e entrega de declarações de inexistência de conflitos de interesses.

Título V - Disposições finais e transitórias

Artigo 38.º - Entrada em vigor e disposições transitórias

83. Conforme já indicado, mesmo num cenário razoável de entrada em vigor de um Regulamento bastante mais aligeirado, a MEO considera que as Empresas devem dispor de tempo e flexibilidade para se adaptarem.

84. Neste sentido, admitindo que são acolhidas as propostas da MEO de simplificar a classificação dos ativos (considerando apenas uma categoria de ativos críticos – ver parágrafo 40 supra) e de recorrer aos procedimentos em vigor nos operadores, a MEO considera que o prazo previsto na subalínea i) da alínea c) do n.º 2 deste Artigo deve ser revisto de 12 para 18 meses.

85. Caso a proposta de simplificação do inventário seja apenas parcialmente aceite pela ANACOM, restringindo-o, por exemplo, às categorias A e B, e seja mantido o nível de exigência do Projeto

de Regulamento quanto aos procedimentos a seguir, então a MEO considera que o prazo previsto na subalínea i) da alínea c) do n.º 2 deste Artigo deverá ser revisto e faseado, prevendo uma primeira fase de 24 meses para os ativos A e uma segunda fase, também de 24 meses, para os ativos B.

86. Por fim, a MEO considera que o prazo previsto na subalínea iii) da alínea d) relativo à adoção de um sistema de controlo de acessos deve ser de 24 meses.

SECURITY AND INTEGRITY OF NETWORKS AND SERVICES

Obligation	Portugal Y/N	Portugal Description	ES Spai Y/N	FR Fran Y/N	BE Belg Y/N	SE Swe Y/N
Assets classification						
Classification of assets in classes of importance/significance	Y	Assets to be classified in 4 classes (A, B, C, D) according to certain characteristics (number of subscribers or accesses or geographic area affected by a failure to operate, level of relevance in the provision of networks and services, interconnection role)	Y		N	Y
Assets inventory						
Build and maintain an inventory of assets	Y	To include assets A, B or C and critical assets to guarantee the integrity of the networks and ensure the continuity of supply of networks and services	Y		Y	Y
Specific detailed information of each asset in the Inventory		Amongst others, we highlight the following:				
	Y	Supported features and services;	Y		Y	Y
	Y	The asset's class (A, B, C) and a description of the potential impact of an interruption or serious disturbance of its functioning;	Y		Y	Y
	Y	Geographical location and identification of entities holding or managing sites;	Y		Y	Y
	Y	Autonomy in case of power failure;	N		N	Y
	Y	Supplies of critical third parties for their operation, including management, operation, security and energy services;	Y		N	Y
	Y	Measures, controls and security records adopted;	Y		N	
	Y	Recording of security incidents that occurred			N	
	Y	Record of the changes made, including the results of the integration and system tests carried out and the restoration plans of the assets	Y		Y	
Send a summary of the inventory to the regulator	Y	Undertakings must send to the regulator a summary of the inventory that should contain for each of the assets: unique identifier, designation, class in which it was classified, geographic location and identification of entities holding or managing the sites.	Y		Y	N
Risk Analysis						
Periodic Comprehensive Risk Analysis	Y	Carry out, at least once a year, a Comprehensive Analysis of the Risks Associated with Class A, B or C, Critical Assets or after a notification of an imminent security breach threat by the regulator.	Y		Y	Y
Periodic Partial Risk Analysis	Y	Carry out a partial risk analysis whenever a security incident occurs; or regarding the assets pertinent for the provision of services to a specific customer, following a notification by the regulator identifying that customer as "relevant"; or regarding the assets identified in the context of civil emergency or civil protection planning.	N		Y	Y
Impacts of the risk analysis		Following each Risk Analysis, undertakings should:				
	Y	Review the assets' classification and, if necessary, reclassify and update the Asset Inventory	N		N	Y
	Y	Adopt appropriate technical and organizational measures including, but not limited to, redundancy, robustness and resilience measures	N		N	Y
	Y	Review and, if necessary, update the General Characterization of Security, the Security Plan and other documentation included in the Safety Dossier.	Y		Y	Y
Redundancy, robustness and resilience						
Ensure redundancy by establishing alternative assets in a different geographic location	Y	Required for class A assets	N		N	Y
In case of redundancy impossibility, undertakings should adopt alternative measures and notify ANACOM of its adoption and the respective rational, including the results of the tests/simulations performed.	Y	Required for class A assets	N		N	Y
Redundancy of links between assets of different classes	Y	Undertakings shall ensure the redundancy of the links between the assets classified in classes A, B or C and, in the case of links between the assets classified in classes A or B, that such links follow different geographical routes.	N		N	Y
Uninterrupted power supply	Y	Undertakings shall ensure that the assets of classes A, B or C are equipped	Y		N	Y

Nota:
As resposta relativas ao UI
não incluiram o preenchim

		with emergency power supply system to enable them to ensure their undisturbed or uninterrupted operation (for a settled minimum number of hours) in case of power supply interruption.						
Tests / Simulations		Undertakings shall carry out tests/simulations, including tests on the operation of emergency power supply systems, at least every six months, recording their performance and the results obtained.	N		Y		Y	
Access control system **Monitoring and control system**								
Periodic review	Y	To be reviewed at least annually and whenever necessary, in particular as a result of the Risk Analysis carried out	Y		Y		Y	
Periodic tests	Y	Undertakings must carry out tests on Access Control Systems and on the Monitoring and Control Systems, at least every six months, in order to protect against unauthorized accesses.	N		Y		Y	
Documentation	Y	Undertakings shall ensure the documentation and recording of the operation of the Access Control Systems and of the Monitoring and Control Systems, including: Threats detected, Security incidents that occured, Alarms generated, The activated measures, The tests carried out, The changes introduced.	Y		N		N	
Training exercises / drills								Y
Elaboration and implementation of an program of training exercises / drills	Y	Undertakings shall prepare an Annual Drill Program	Y		Y			
Reports	Y	Undertakings shall prepare reports on the implementation of the Annual Drill Program, including a description of the results obtained.	N		Y		Y	
Relevant customers								N
"Relevant" customers	Y	For the purpose of this regulation, relevant customers are entities that provide relevant services to society such as the entities managing the Integrated System of Emergency and Security Networks or the National Internal Security Network. ANACOM can also notify undertakings of the identification of other "relevant" customers, such as the providers of essential services (water, electricity, etc.).	N		N			
Notification of security and integrity incidents related to "relevant" customers	Y	Undertakings shall notify ANACOM of any incident with duration >= 30m related to network elements which may impact the provision of services to "relevant" customers.	N		N		N	
Documentation								N
General Characterization of Security	Y	Undertakings must prepare and send to the Regulator the General Characterization of Security (including the description of the control systems in place, the contact information of the Security Officer and of the Permanent and Alternative Contact Person)	Y		N			
Security Plan	Y	Undertakings must prepare a Security Plan and keep it updated, with annual reviews or whenever necessary as a result of the risk analyses carried out.	Y		Y		Y	
Security Report	Y	Undertakings must prepare and submit to ANACOM an Annual Security Report on the activities performed concerning risk analysis, training exercises / drills, audits, results obtained, analysis of the incidents with the greatest impact. The report must also include a summary of the changes and improvements introduced to the Security Plan and the Annual Drill Program for the following year.	Y		N		Y	
								N

Please find attached the answer to your enquiry on network security requirements.
Put short, the Spanish General Law on Telecommunications foresees that the competent ministry (Ministry for the Digital Agenda) must issue regulations establishing mechanisms for telecom operators to guarantee an "adequate level of security" of their networks and minimise the impact of any security incidents. **However there is no maximum timing for adoption of such implementing regulations, which are not in place as of** Telecom operators are subject to the general obligations on the protection of critical infrastructure, which mostly impose minimum planning and notification requirements (**the detail of how security is to be guaranteed is left to the operator, with some recommendations of best practices**). The national critical infrastructure catalogue is confidential (for security reasons), so I cannot tell you if all or only some of the telecommunications infrastructure/services are considered critical.

I would like to give you some background as the elements I have inserted in your questionnaire may

General regime for all operators is in the Electronic Communications Code. It is not deeply detailed. It provides that operators must take all appropriate technical and organisational measures to ensure the security of their network and services at a level appropriate to the existing risk.

You also have some provisions dealing in particular with national security:

- have the technical and human resources to solve issues in case of failure, destruction of information;
- be able to cope with public security and national defence needs in case of emergency, crisis;
- set specific connections reserved for public authorities as agreed with relevant authorities in case of emergency, crisis

Network security breaches must be reported to the minister of interior, who informs the minister in charge of telecommunications and relevant security services if necessary. If the origin of the breach of security and/or the integrity loss is likely to be a cyber-attack, the national agency of security of information systems (ANSSI) must also be informed by the operator. For security breach due to power failure, storm damage etc., telecom regulator ARCEP is informed by the Minister of interior/telecoms

Beside this general regime, there is a more targeted regime for what is called operators of vital importance for the country (Defence Code, art. 1332-1). Such operators have activities and manage infrastructures, information systems of major importance for the country (i.e. unavailability or destruction would have major consequences on economy, security, health ...). Several sectors are covered: energy, telecom, water, finance,

An Ordinance of Nov. 26, 2016 (prepared by the French Information Systems Security Agency - ANSSI) set specific security rules for the security of information systems of electronic communications operators (maintenance, detection of issues, alerts, etc.). Main problem is that all the details for those measures are set in annexes which are not public (only notified to operators designated as managing information systems of vital importance). **The operators under this regime are also not known: they are designated by the**

In your questionnaire, I have plugged some data coming from this specific regime, which seems to be the more detailed one, and that are similar to the Portuguese regime. Nevertheless, I would not say that it is equivalent. In addition, since a lot of information is secret, it is hard to fully answer the questionnaire

Javier and James asked me to give my input on the regulation in Belgium related to the security and integrity of public electronic communication networks and services.

I've filled in your table in attach.

I have researched the applicable regulation only (telecom law, secondary law and Royal Decrees) as well as Anything that is not explicitly mentioned, I've put a 'N'.

Nowhere the regulation mentions ISO standards or ENISA guidelines, but that does not mean that in practice **It seems the Belgian regulation is less descriptive than the Portuguese proposal. It relies on the sense of responsibility of operators and informal rules agreed within the sector and between sector and government/regulator.**

Please find attached an overview of the measures and obligations related to the security and integrity of public electronic communication networks and services that have been mandated by the Swedish regulator

Here is the link to PTS regulations on network security:
http://www.pts.se/upload/Foreskrifter/Tele/PTSFS%202015-2%20-%20Drifts%C3%A4kerhet.pdf
The regulations entered into force on January 1, 2016, but **specific obligations related to redundancy and uninterrupted power supply will apply after 5 years from the date of the adoption**, i.e. from June 2020.

I should perhaps add that we decided to send you details on Sweden because the scope of the obligations imposed by PTS is very similar to those proposed by ANACOM – **with the exception perhaps of the extensive reporting requirements.**

Regarding the situation in the UK, Ofcom published in 2014 guidance to communications providers on security

https://www.ofcom.org.uk/__data/assets/pdf_file/0021/51474/ofcom-guidance.pdf

The relevant parts are:

Section 3 – protecting security – pages 4 to 9
Section 5 – auditing and enforcement – page 20

In particular, Ofcom refers to ISO 27001 and the ENISA Technical Guidelines on security measures.

I checked with Ofcom, there has been no further update to this guidance and there is also no additional more detailed guidance.

For Ireland, **I cannot find anything so detailed as seems to be the case (being proposed) in Portugal.** ComReg consulted on and published guidelines in 2014 (https://www.comreg.ie/csv/downloads/ComReg1402.pdf) but these focus much more on the thresholds for incident reporting rather than the "auditing" type provisions on general security measures that are covered

2.2 Management of the integrity of networks

ComReg is not being prescriptive *as to the precise measure that operators should take to manage risk in respect of network integrity and security but notes its responsibility to monitor these activities.*

ComReg ***may*** *require Operators to provide information that would be used to assess the security and integrity of the services and networks of that Operator and where necessary to submit to a security audit that would be carried out by an independent professional body nominated by ComReg pursuant to*

Best regards

Peter

6 Conclusion on Minimum Security Standards

126. Operators should familiarise themselves with ENISA guidelines for Minimum Security Measures[10]. ComReg will consider the guidelines in this document as well as other specific circumstances when assessing an Operator's compliance with its obligations. If these guidelines change ComReg will expect Operators to take such changes into consideration when determining appropriate technical and organisational measures to appropriately manage the risks posed to integrity and security of networks and services.

127. ENISA proposed various standards that Operators may use and ComReg notes that an Operator may use alternative standards which achieve the same objective.

128. ENISA advises that Operators should perform risk assessments, specific for their particular setting, to determine which assets fall under the scope of security measures (the assets to which they should be applied). These assets include assets which, when breached and or failing, can have a negative impact on the security or continuity of electronic communications networks.[11]

129. 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.

130. As explained in this document ComReg will use reports from Operators as one of the tools for monitoring compliance by Operators with their obligations under Regulation 23 (1). Other formal powers are available to ComReg for information gathering including the use of external audits and ComReg will use such powers as it considers appropriate.

The situation in Italy is similar to Spain.

The general requirements under art. 13a of the EU Framework Directive are transposed in art.16-bis of the Electronic Communications Code 259/2003.

This article foresees that the Ministry of Economic Development will "identify" appropriate technical and organisational measures to appropriately manage the risks posed to security of networks and services, and

After that, providers of public electronic communications networks/services (PECN/S) should adopt these

However, so far, the ministry has not issued (or at least made public) any such required technical and organisational measures. The law does not set any deadline for it.

As part of the "national cyber security and information security plan", on Jan. 24, 2013 the government issued a Cyber Security Directive with a wide scope of *"ensuring national interests in relation to material and immaterial critical infrastructures, with particular regard to cyber and information security"* . (Legislative Decree 61/2011 transposed Directive 2008/114/EU on critical infrastructures but same as the directive, it

Art. 11 of the Italian Cyber Security Directive explicitly requires PECN/S to adopt *"best practices and measures to ensure cybersecurity"* in line with art. 16-bis of the Electronic Communications Code. But as the ministry has not taken the first step to identify those measures (see above), this provision has not been implemented either. Or at least none of the main telecoms operators has published any such best practices.

In practice, the main telecoms operators seem to be ISO certified, see for example TIM (ISO 27001) and Fastweb (ISO 22301, 27001, 27018).