[redacted]

From: [redacted] <[redacted]@deloitte.pt>
Sent: 14 de março de 2017 22:02
To: regulamento.seguranca@anacom.pt
Cc: [redacted]
Subject: Comentários da Deloitte ao Projeto de regulamento relativo à segurança e à integridade das redes
Attachments: Comentários da Deloitte ao Projeto de regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas 4.pdf

Exmos Srs.

No âmbito da consulta pública sobre o projeto de regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas, vimos pelo presente apresentar em anexo os nossos comentários e observações.

Aproveitamos para manifestar a nossa total disponibilidade e interesse em dar o nosso contributo sempre que julguem podermos acrescentar valor.

Com os melhores cumprimentos,

[redacted]
Deloitte
Av. Eng. Duarte Pacheco, 7, 1070-100 Lisbon, Portugal
[redacted] www.deloitte.pt

Deloitte

Comentários da Deloitte ao Projeto de regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas

No passado dia 29 de dezembro de 2016, a ANACOM aprovou o projeto de regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas, o qual foi publicado na Série II do Diário da República n.º 7/2017 - Aviso n.º 459/2017.

No âmbito do processo de consulta pública promovido pela ANACOM sobre este projeto de regulamento, nos termos do Artigo 10.º dos Estatutos da ANACOM, Artigos 98.º e seguintes do Código do Procedimento Administrativo e Artigos 8.º E e 54.º C, n.º 4 da Lei das Comunicações Eletrónicas, vem a Deloitte apresentar os seus comentários a este documento, esperando contribuir para a construção de um quadro regulatório robusto e eficiente em matéria de segurança e integridade nas redes e serviços.

I. Comentários Prévios

Em primeiro lugar, a Deloitte congratula a ANACOM pela aprovação de um projeto de regulamento em matéria de segurança e integridade das redes e serviços, no sentido de garantir a transparência, eficiência e segurança jurídica nas medidas técnicas de execução e requisitos adicionais a cumprir pelas empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público e nos procedimentos aplicáveis às exigências de comunicação de violações de segurança ou perdas de integridade das redes com impacte significativo no funcionamento das redes e serviços daqueles operadores.

II. Comentários ao projeto de regulamento

De forma sistematizada, a Deloitte apresenta os seguintes comentários:

REFERÊNCIA AO TEXTO PROPOSTO	COMENTÁRIOS
Artigo 4º, 2 a) "*Riscos, ameaças ou vulnerabilidades, comuns ou de efeito em cascata*;"	No sentido de clarificar, sugerimos a inclusão nas Definições (Artigo 3º) de uma explicação sobre o que se entende por vulnerabilidades em cascata (que potenciam efeito em cascata).
Artigo 5º, 1 a) "*As empresas 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*;"	Compreendendo a especial relevância e contexto atual onde as redes se encontram interligadas, poderá fazer sentido não restringir o texto final apenas às "redes interligadas" mas a todas aquelas a que se aplique este artigo, eventualmente dando particular relevância a estas.
Artigo 6º, 2	Avaliar a adequação deste parágrafo no sentido de clarificar que, mediante os resultados da análise de risco, a empresa deverá adequar as medidas definidas nos Artigo(s) 10º ao 15º,

"*Para efeitos do disposto na alínea b) do número anterior, as medidas a adotar ao abrigo do disposto nos artigos 10.º a 15.º devem ser reforçadas pelas empresas sempre que necessário e na medida adequada em resposta aos resultados das Análises de Risco realizadas*."	por forma a assegurar a correta mitigação dos riscos identificados e de acordo com definido no Artigo 9º.
Artigo 6º, 2 "*Para efeitos do disposto na alínea e) do n.º 1, as empresas devem estabelecer e manter uma estrutura apropriada de funções e responsabilidades de segurança, bem como assegurar que estão dotadas da capacidade técnica necessária, nomeadamente ao nível dos recursos humanos, dos ativos e dos fornecimentos por terceiros, para garantir o cumprimento das suas obrigações em matéria de segurança e integridade das redes e serviços, nos termos previstos na lei e no presente regulamento*."	Avaliar a pertinência de assegurar, através da realização de auditorias independentes, que as empresas avaliam e garantem o cumprimento dos requisitos aqui estabelecidos e aos quais estão obrigadas, ao nível dos serviços prestados por terceiros. A responsabilidade pela salvaguarda da segurança e integridade das redes e serviços de comunicações eletrónicas caberá sempre à empresa prestadora de serviço, devendo por isso ser responsável por salvaguardar que os terceiros, a quem possa confiar parte da cadeia de suprimento, estão devidamente alinhados com este regulamento e cumprem na exata medida do seu impacto.
Artigo 7º, 8 "*As empresas devem ainda classificar os ativos identificados no âmbito do planeamento civil de emergência ou de um plano de emergência de proteção civil que a ANACOM indique através de notificação às mesmas, a qual inclui*:"	Sugerimos a seguinte redação para este parágrafo "*As empresas devem ainda classificar os ativos que, tendo sidos identificados (…), sejam indicados e comunicados pela ANACOM às empresas e de acordo com o a classe indicada. A ANACOM notificará as empresas neste sentido, onde incluirá a seguinte informação*:"
Artigo 8º, 1, a) "*Os ativos classificados nas classes A, B ou C;*"	Avaliar a pertinência da inclusão da globalidade dos ativos no inventário, de forma a assegurar que o universo está compreendido. A sua não inclusão poderá resultar na: (i) análise daqueles que numa primeira fase se entenda relevantes sem olhar aos demais; (ii) deste modo, na altura da inventariação poder-se-á não atender ao universo; (iii) a classificação apenas de parte do universo poderá excluir à partida ativos da análise de risco; (iv) com a revisão da avaliação do risco o atual texto parece prever a possibilidade da eventual alteração da classificação, para tal será importante ter inventariados os ativos de classe D; (v) na avaliação/ auditoria será importante que se avalie a correta classificação dos ativos, nomeadamente os de classe D.
Artigo 8º, 1, b) "*Os ativos críticos para a continuidade do funcionamento das suas redes ou serviços*."	Poderá haver uma redundância entre este parágrafo e o anterior, na medida em que poderá não ser clara a diferença entre os "ativos críticos" e os de classe A, B, C, ou D. Avaliar a pertinência da simples indicação de necessidade de inclusão da totalidade dos ativos no inventário.
Artigo 8º, 2, c), iii) "*Medidas, controlos e registos de segurança adotados;*"	Avaliar a pertinência de se passar esta alínea para um nível superior (i.e. alínea d), na qual as empresas devam descrever as medidas, os controlos e os registos de segurança que tem associados a cada um dos ativos.

Artigo 8º, 3 "*As empresas devem elaborar o Inventário de Ativos no prazo de 60 dias úteis a contar da data de início de atividade*."	Rever a redação deste parágrafo, de forma a esclarecer o que se entende por início de atividade. No Artigo 38º c) está estipulado que as empresas tem até um ano.
Artigo 9º, 1, a) "*De âmbito global, em relação aos ativos classificados ou classificáveis nas classes A, B ou C ou críticos para a continuidade do funcionamento das suas redes ou serviços*:"	Avaliar a relevância da avaliação dos ativos de classe D também. Será importante que as empresas tenham mecanismos para, quando aplicável, poderem reequacionar/rever a classificação de um determinado ativo e o risco associado (e.g. C para D, D para C)
Artigo 9º, 3, a), iii) "*De ataques maliciosos*;"	Avaliar a pertinência de se substituir a expressão "ataques maliciosos" por "atos maliciosos" (estes incluem os ataques)
Artigo 9º, 4, a) "*O histórico de situações extraordinárias ocorridas*;"	Avaliar a redação atual com o objetivo de clarificar o que se entende por "situações extraordinárias". Serão eleições, referendos, eventos com pico de acesso a serviços, etc.? Qual a diferença para incidentes de segurança?
Artigo 9º, 4, e) "*A garantia de acesso aos serviços de emergência*;"	Com o objetivo de clarificar, sugerimos a inclusão nas Definições (Artigo 3º) de uma explicação quanto a "serviços de emergência"
Artigo 9º, 6, a) "*Rever a classificação dos ativos e, se necessário, proceder à sua reclassificação e à atualização do Inventário de Ativos*;"	Sugerimos que sejam considerados os ativos de classe D na revisão da classificação e inventário
Artigo 9º, 7, d) "*O acesso aos serviços de emergência*;"	Com o objetivo de clarificar, sugerimos a inclusão nas Definições (Artigo 3º) de uma explicação relativamente ao que se entende por "serviços de emergência"
Artigo 9º, 8 "*Para efeitos do disposto no presente artigo, a ANACOM pode, caso assim o entenda necessário, emitir orientações com vista a uma harmonização da matriz de risco a adotar pelas empresas*."	A menção à "matriz de risco" é feita pela primeira vez neste parágrafo. . Esta não se encontra nas Definições nem é explicada a sua utilidade ou funcionalidade.
Artigo 10º, 1, a) "*Assegurar a sua redundância mediante o estabelecimento de ativos alternativos em local geográfico distinto*;"	O texto não estabelece o que se entende por "local geograficamente distinto" ou distância a que possa corresponder.
Artigo 12º, 2 "*Em especial no caso de alterações físicas ou lógicas aos ativos classificados nas classes A ou B, as empresas devem*:"	Importante avaliar o impacto das alterações realizadas ao nível dos ativos classificados com C e D, nomeadamente ao nível dos ativos classificados com A e B (interdependências).
Artigo 12º, 2, a) "*Assegurar a realização de testes de integração e de sistema antes da introdução da alteração*;"	Avaliar a pertinência de complementar o texto desta alínea com a recomendação de os testes se realizarem em ambiente não produtivo.

Artigo 13º, 2 "*Os Sistemas de Controlo de Acessos devem*:"	Avaliar a pertinência de se adicionar alínea para assegurar que o sistema de controlo de acesso permita a gestão de acessos de emergência.
Artigo 13º, 3 "*As empresas devem realizar testes aos Sistemas de Controlo de Acessos, com uma periodicidade mínima semestral, com vista à proteção contra acessos não autorizados*."	Avaliar a pertinência de detalhar os objetivos destes testes (como por exemplo: identificar os acessos que não estão alinhados com as necessidades e/ou responsabilidades atribuídas, nomeadamente através da análise de tentativas de acesso falhadas, acessos mal atribuídos, acessos desatualizados, etc.)
Artigo 14º, 3 "*As empresas devem realizar testes aos Sistemas de Monitorização e Controlo, com uma periodicidade mínima semestral*."	Avaliar a pertinência de inclusão de um artigo a clarificar o que se entende por "sistema de monitorização e controlo" e, adicionalmente, esclarecer em que medida estes sistemas são ativos (e.g. NOC, SOC, etc.)
Artigo 16º "*As empresas devem comunicar aos seus clientes previstos no n.º 6 do Artigo 24.º, com conhecimento da ANACOM, as medidas adotadas na sequência de incidentes de segurança ou em reação a ameaças ou a vulnerabilidades*."	Sugerimos que se remova a parte final deste parágrafo: "*ou em reação a ameaças ou a vulnerabilidades*". Se necessário, avaliar a pertinência de clarificar o que se entende por "incidente de segurança", onde se incluem as tentativas.
Artigo 17º, 1, h "*A identificação e os contactos do Responsável pela Segurança, incluindo*:"	Avaliar a pertinência de se fazer referência Artigo 20º no texto deste parágrafo.
Artigo 20º, 1 "*As empresas devem estabelecer uma função de Responsável pela Segurança, o qual, entre os demais deveres previstos no presente regulamento, é responsável*:"	Avaliar a pertinência de se associar a este responsável a execução/contratação das auditorias e aplicação de demais requisitos em articulação com as áreas operacionais da empresa.
Artigo 20º, 1, b), "*Pela gestão do sistema de gestão de segurança*;"	Avaliar a pertinência de se clarificar/definir o que se entende por "sistema de gestão da segurança". Avaliar, adicionalmente, a menção à relevância da introdução de melhores práticas e obtenção de certificação nas mesmas, enquanto fator de confiança (ver exemplo do Regulamento Geral de Proteção de Dados (EU 679/2016)
Artigo 20º, 2 "*As empresas que não estejam estabelecidas na União Europeia ou no Espaço Económico Europeu e que detenham ativos classificados nas classes A, B ou C devem assegurar que o seu Responsável pela Segurança se encontra aí domiciliado*."	Não é claro se este responsável deve estar estabelecido em Portugal ou se poderá estar estabelecido em qualquer outro país da União Europeia ou Espaço Económico Europeu. Avaliar a pertinência da obrigação deste responsável estar localizado em Portugal, sempre que as decisões sobre a gestão, alterações, etc. relativas aos ativos sejam tomadas em Portugal. O texto do regulamento não deixa claro qual o papel deste responsável na interação com a ANACOM, e estando localizado fora de Portugal, como será realizado o controlo da sua atuação.

Artigo 30º, 2 "*Para efeitos do disposto no número anterior e até ao dia 30 de junho de cada ano, a ANACOM publica, no seu sítio institucional na Internet, as referências das normas, especificações e recomendações a que devem conformar-se as Auditorias do ano seguinte*."	Não é claro o período relativamente ao qual deverá incidir a auditoria (e.g. ano anterior, ano corrente). Avaliar a pertinência de se definir um prazo para a adoção de alterações às referências (i.e., quando passam a ser aplicáveis novas referências? E para que período?)
Artigo 31º, 2 "*As empresas devem assegurar que as Auditoras não são seus fornecedores para outros serviços que não sejam a realização de auditorias externas e independentes e que entregam declarações de inexistência de conflitos de interesses em seu nome e em nome de todos os colaboradores envolvidos*."	As empresas devem assegurar que não existem conflitos de independência das auditoras considerando a legislação vigente nesta matéria.
Artigos 34º, 35º e 36º	Os prazos aqui apresentados parecem-nos demasiado otimistas, nomeadamente porque não leva em consideração a necessidade de as empresas precisarem de estabelecer os âmbitos e contratualizarem as auditorias com terceiros.
Artigo 35º, 6 "*Compete à ANACOM a aceitação do Relatório de Auditoria, podendo, para o efeito, solicitar à empresa a prestação dos esclarecimentos necessários e o suprimento de deficiências existentes*."	O relatório de auditoria corresponderá ao resultado do trabalho de auditoria realizado, da responsabilidade do auditor. Avaliar a pertinência da definição de necessidades específicas adicionais serem partilhadas na fase de aceitação da auditoria.

Março de 2017