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

Artigo 1.º: Objeto

- Entendemos que o âmbito do regulamento é demasiado genérico, devendo ser limitado à vertente da disponibilidade dos serviços e restringido a situações que acarretam a interrupção de serviços, tendo em conta o referido no nº 2 do artigo 54º-C e no artigo 54º -D da Lei das Comunicações Eletrónicas.
- Deve igualmente ser clarificado o objeto em termos dos serviços a que se aplica o Regulamento, devendo ser tida em conta a importância desses serviços para os cidadãos.

Artigo 2.º: Âmbito

- Consideramos que não é possível assegurar o cumprimento das obrigações de segurança e integridade das redes de forma igual em situações normais e em situações de força maior, pelo que deve ser referido que no segundo caso, as empresas envidarão os esforços para assegurar essas obrigações tendo em conta os eventuais impedimentos decorrentes dessas situações de força maior. Assim propomos que no ponto 2, se altere a redação para o seguinte: "As empresas devem cumprir as suas obrigações (…) de um modo adequado às condições climáticas, de desastre natural…",
-

Artigo 7º Medidas técnicas de segurança

- No que se refere ao ponto 1 entendemos que a obrigação de aplicação generalizada dos níveis de sofisticação 1 e 2 para a prossecução de todos os objetivos de segurança constantes do Anexo, deveria ser ajustada a uma lógica de gradualismo e de uma análise custo/beneficio que justifique a passagem do nível 1 para o nível 2. Deverá ser assim definido um período em que seja obrigatório apenas o nível 1 e que permita fazer essa análise custo/benefício da passagem para o nível 2 (e 3), definindo-se depois um período (nos casos em que se justifique) a passagem ao nível 2.
- Em relação ao ponto 3 parece-nos existir redundância entre algumas medidas específicas e os 25 SO definidos que deveria ser minimizada

Art.º 8: Classificação de ativos

- Em relação ao nº 3, consideramos que a alínea c), ao remeter para a alínea f do nº 2 do artigo 21 implica que sejam considerados os ativos associados à prestação de serviços aos operadores de serviços essenciais e de infraestruturas criticas o que implica, face à abrangência geográfica destas entidades, que quase todos os ativos de um operador que tenha este tipo clientes seja classificado como de Classe A, o que seria eventualmente o caso da Fibroglobal, embora, nos termos dos outros critérios, nomeadamente em termos do número de clientes/acessos afetados, pelo contrário, teríamos poucos ativos classificados como de classe A. Pelo exposto e pela contradição entre os dois tipos de critérios, consideramos que não se deve aplicar o previsto na alínea c).
- Também nos levanta reservas a alínea e) do nº 3, por implicar que tenhamos de estar dependentes da apreciação da ANPC/ANACOM na definição da criticidade de um determinado ativo. Aceitamos neste âmbito que possa haver uma indicação/recomendação, mas não uma obrigação.

Art.º 9: Inventário de ativos

- É nosso entendimento que só devem ser inventariados os ativos críticos, pelo que os ativos da Classe C devem ficar excluídos deste processo.
- No caso dos ativos críticos, não nos parece que se justifique a alínea d) do ponto 2. e preocupa-nos a obrigação de transmissão dessa informação à Anacom, dadas às implicações daí resultantes em termos da segurança dos dados.
- Os requisitos do ponto 3 parecem-nos excessivos se entendidos como obrigatórios. Deverão ser entendidos como indicativos.
- Estamos em desacordo com a obrigação de transmissão de informação à Anacom prevista no ponto 5, nomeadamente pelos motivos já expostos em termos de segurança de informação e também pela não justificação da mesma.

Art.º 12: Exercícios

- Para clarificação, entendemos que a periodicidade recomendada (e não máxima) deve ser definida como de dois em dois anos.

Art.º 13: Informação aos clientes

- A obrigação de comunicação aos clientes relevantes, nos termos que estão definidos no nº 5 do artigo 21º, em particular das alíneas d) e e) parece-nos muito abrangente e discricionária. Estas alíneas deveriam ter caráter indicativo e não obrigatório, bem como no que se refere à obrigação de comunicação prévia à Anacom.

Art.º 19: Relatório anual de segurança

- Deve ser excluída a obrigação de disponibilizar estatísticas trimestrais dos incidentes "sem impacto significativo". Estes incidentes "sem impacto significativo" não são relevantes face às regras e patamares definidos no Regulamento
- Deve ser opcional a indicação do programa de exercícios previstos para ano civil seguinte.
- Entendemos que não se justifica fornecer a informação prevista na alínea c), face à informação disponibilizada de forma elementar.

Art.º 21: Circunstâncias

- No que respeita ao ponto 2, alíneas b) e f) entendemos que as obrigações de comunicar violações de segurança e perdas de integridade que envolvam entidades críticas para a segurança nacional devem ser asseguradas diretamente por estas entidades.

Art.º 22: Formato e procedimentos

- Existem constrangimentos em garantir o nº7 do artigo 22º, sobretudo no prazo de duas horas após o fim da ocorrência, uma vez que o apuramento concreto das freguesias e respetivos concelhos é um processo complexo e moroso, particularmente quando são afetados determinados segmentos de rede ou tecnologias, pelo que a indicação concreta das zonas afetadas deverá ser limitada à notificação final.

Art.º 24: Notificação ao público

- É nosso entendimento que o prazo previsto no nº 1, alínea c) deve se manter no valor de 4 horas úteis, como já tinha sido aceite. Voltar ao valor de 1 hora útil não é exequível.

Art.º 25 a 33: Auditorias

- Relativamente ao artigo 29º e sem prejuízo do cumprimento dos deveres de colaboração nele previstos entendemos que qualquer contacto que venha a ser realizado com os fornecedores relevantes ao nível da segurança e integridade das redes e serviços deverá ser feito por nosso intermédio e deverá acontecer apenas se existirem dúvidas fundamentadas sobre os resultados da auditoria.
- Relativamente ao artigo 31º, entendemos que os elementos solicitados nas alíneas a), b) e c) do nº1 do artigo 31º não devem de disponibilização obrigatória na fase de pré-auditoria e/ou deve ser acautelada a possibilidade de revisão destes elementos em fases posteriores.
- Relativamente ainda ao artigo 31º entendemos que o prazo de realização das auditorias deve ser superior a 2 anos. De dois em dois anos parece-nos um prazo demasiado curto, com custos elevados e sem justificação.