Resposta conjunta da NOWO e ONI à consulta pública sobre a 2ª versão do Projeto de Regulamento relativo à Segurança e à Integridade das Redes e Serviços de Comunicações Eletrónicas

03.10.2018

1. Enquadramento

Em 29 de Dezembro de 2016 a ANACOM publicou a 1ª versão do Projeto de Regulamento relativo à Segurança e à Integridade das Redes e Serviços de Comunicações Eletrónicas ("Regulamento"), o qual foi submetido a consulta pública após publicação na 2ª série do Diário da República, a 10 de Janeiro de 2017.

O Regulamento abrangia os seguintes temas:

- Medidas técnicas de execução e requisitos adicionais
- Notificação de incidentes ao Regulador
- Divulgação de incidentes ao Público
- Auditorias de segurança

As empresas de comunicações eletrónicas ("operadores"), nas suas respostas individuais e na resposta conjunta via APRITEL à consulta pública, assinalaram um conjunto de problemas na 1ª versão do Regulamento, de que se destacam as seguintes:

- Classificação e cadastro de ativos com grande complexidade
- Exigências muito elevadas das medidas técnicas e requisitos adicionais, com adoção do nível de sofisticação mais elevado
- Eram definidas medidas operacionais a adotar pelos operadores, em vez de se definirem os objetivos de segurança e deixar aos operadores a opção pelas medidas operacionais adequadas
- Obrigações de envio de informação à ANACOM muito exigentes e que criavam potenciais problemas a nível de segurança e confidencialidade da informação
- Obrigações complexas e excessivas a nível da análise dos riscos
- Periodicidade excessiva dos exercícios de segurança, com potencial disruptivo a nível operacional
- Regime transitório com prazos demasiado curtos face à complexidade das exigências

Tendo em conta os comentários recebidos, a experiência adquirida com as notificações sobre incidentes de segurança e os resultados do Grupo de Trabalho sobre Incêndios (que a ANACOM criou e coordenou, tendo apresentado o relatório final a 29 de Maio de 2018), a ANACOM decidiu proceder à revisão do Regulamento, tendo agora publicado uma 2ª versão, que submeteu a consulta pública.

A NOWO Communications S.A. ("NOWO") e a ONITELECOM – Infocomunicações, S.A. ("ONI") vêm por este meio, apresentar a sua resposta conjunta à consulta pública sobre a 2ª versão do

Regulamento. Esta resposta compreende uma secção de comentários gerais, à qual se seguem comentários específicos aos vários artigos do Regulamento.

2. Comentários gerais

A ANACOM foi sensível a muitos dos argumentos apresentados pelos operadores na consulta pública à 1ª versão do Regulamento, tendo introduzido extensas alterações nesta 2ª versão, no sentido de endereçar os problemas que tinham sido assinalados. Saúda-se a atitude e o esforço do Regulador a este propósito.

Das alterações introduzidas, destacam-se as seguintes.

A aproximação prescritiva da 1ª versão é substituída pela definição de objetivos de segurança ("OS") de acordo com as recomendações da ENISA, o que acolhe totalmente uma das principais críticas dos operadores à 1ª versão do Regulamento

O nível de sofisticação a adotar para as medidas técnicas de execução é reduzido para o nível 2. Embora esta redução acolha em parte uma crítica dos operadores à 1ª versão do Regulamento, continua a ser um nível de exigência muito elevado, que não deixará de ter impacto relevante na operação e investimentos dos operadores. Consideramos que seria mais adequado que se adotasse o nível 1 de sofisticação como exigência geral e se definisse uma calendarização de evolução para níveis mais exigentes que permitisse diluir no tempo os necessários investimentos, minimizando assim o impacto financeiro sobre os operadores. O período de evolução deveria resultar de uma avaliação global de risco e de uma análise custo-benefício dos níveis de sofisticação das medidas técnicas de execução, o que não foi feito.

Apesar do que se refere no ponto anterior, o Regulamento permite algum grau de flexibilidade aos operadores ao admitir que, com justificação numa análise de risco, a ANACOM possa autorizar o nível 1 de sofisticação para algumas medidas técnicas de execução. De novo, embora se reconheça que o Regulador foi parcialmente sensível aos argumentos dos operadores nas suas respostas à consulta sobre a 1ª versão do Regulamento, esta flexibilidade é dependente de um esforço elevado de justificação por parte dos operadores, pelo que se defende, em alternativa, a aproximação referida no ponto anterior de adoção do nível de sofisticação 1 e evolução faseada para níveis mais sofisticados com base numa análise de riscos que justifique essa evolução.

São definidas 11 medidas específicas obrigatórias, que são pormenorizadas nos artigos 8º a 19º do Regulamento. Alerta-se que poderá existir alguma sobreposição dessas medidas com as medidas técnicas de execução associadas aos OS listados no Anexo do Regulamento, pelo que se sugere uma revisão no sentido de minimizar tais sobreposições.

São eliminados os anteriores artigos relativos a:

- Medidas de redundância, robustez e resiliência
- Procedimentos de gestão de alterações
- Sistemas de controlo de acessos
- Sistemas de monitorização e controlo

- Caracterização geral de segurança
- Dossier de Segurança

Saúdam-se estas alterações, pois permitem eliminar muito do caráter prescritivo e da complexidade da 1ª versão do Regulamento e que tinham sido alvo de fortes reticências dos operadores

Procedeu-se a uma simplificação da classificação de ativos. Passam a existir dois tipos de ativos críticos (novas classes A e B) e uma classe de ativos não críticos (nova classe C):

  - Classe A – ativos classificados como críticos por disposição do Regulamento
  - Classe B – ativos classificados como críticos por análise do operador
  - Classe C – ativos não críticos

A nova classe A resulta da fusão e simplificação das classes A e B da 1ª versão do Regulamento. Apesar da aparente simplificação, constata-se que a nova definição implica que os principais operadores do mercado deverão acabar por ter vários ativos de classe A.

Por seu lado, o inventário de ativos é simplificado, passando a incluir informação dependente do tipo de ativo (as classes A e B exigem mais informação que a classe C) mas incluindo, também, ativos da classe C. Não se compreende a necessidade de inclusão no cadastro de ativos da classe C, dado que não são ativos críticos.

Na nova versão do Regulamento, as obrigações relativas a "análise de riscos" foram reduzidas a uma obrigação de revisão da metodologia de gestão de riscos. No entanto, não faz sentido impor-se uma obrigação de revisão da metodologia de gestão de riscos, a qual constitui a base de toda a análise de riscos. O que faz sentido é proceder-se à revisão periódica da análise de riscos, de forma a determinar a adequação das medidas técnicas de execução implementadas face ao cenário de risco que o operador enfrenta.

Alterou-se, ainda, a periodicidade dos exercícios de segurança, que passa para um máximo de dois anos. Saúda-se esta alteração, dado o grande impacto operacional de exercícios anuais previstos na 1ª versão do Regulamento. No entanto, considera-se que mesmo uma periodicidade de dois anos poderá ser excessiva, pelo que se sugere uma periodicidade de três anos.

No que diz respeito às notificações de incidentes de segurança à ANACOM, considera-se que a indicação de áreas afetadas ao nível da freguesia introduzirá um nível de complexidade elevado, já que não há um mapeamento imediato e simples da estrutura de rede com estas divisões administrativas, não sendo evidentes os ganhos daí decorrentes para a gestão dos impactos dos incidentes. Isto também se reflete na disponibilização de informação sobre incidentes ao público, onde a apresentação da localização dos incidentes sobre um mapa de freguesias implica desenvolvimentos de sistemas, com consequentes custos, sem que daí advenham ganhos efetivos para o que realmente interessa aos clientes, que é a resolução rápida e eficaz dos incidentes e consequente reposição dos serviços. Assim, advoga-se a manutenção do regime atual de identificação de impactos a nível de concelhos.

Por outro lado, a comunicação ao público de informação sobre incidentes passa a ter de ser feita em regime contínuo, no máximo de uma hora linear após comunicação do incidente à ANACOM. Dado que as comunicações ao público implicam sempre a intervenção das equipas de Comunicação /

Public Relations dos operadores, tal disposição obriga a que essas equipas passem a ter de estar disponíveis em permanência, 24 horas por dia, 7 dias por semana, como se de equipas de intervenção técnica se tratassem. Isto é totalmente desproporcionado, pelo que se defende a manutenção do atual regime de comunicação ao público.

A nível das auditorias constata-se que, por força da definição dos ativos classe A, estas serão, na prática, obrigatórias para os principais operadores nacionais. Apesar de algumas simplificações processuais introduzidas e do alargamento dos prazos, o procedimento definido para as auditorias continua a ser bastante burocrático, pelo que se sugere uma simplificação. Também se defende que devem ser as equipas auditoras a estar sujeitas a rotatividade e não as empresas auditoras, aliás em linha com o que estas empresas já praticam, dado que procedem à rotatividade das suas equipas auditoras num mesmo operador. Por outro lado, entende-se que os elementos da ANACOM que acompanhem as auditorias devem, por razões de equidade, estar sujeitos aos mesmos requisitos que os elementos integrantes das equipas auditoras.

Por fim, continua a entender-se que devem ser minimizados os envios de informação sensível sobre ativos dos operadores para a ANACOM, sem prejuízo do Regulador poder sempre ter acesso à informação que considere necessária nos próprios sistemas e registos dos operadores. Nesse sentido, considera-se que o sistema de informação que o Regulamento menciona e que será desenvolvido para troca de informação entre operadores e ANACOM deverá estar limitado na sua utilização às notificações sobre incidentes de segurança, auditorias e relatório anual de segurança, não se incluindo informação cadastral ou outra informação sensível sobre os ativos críticos do operador.

3. Comentários específicos

Nas secções seguintes apresentam-se comentários específicos e mais detalhados a vários artigos do Regulamento.

3.1. Âmbito (Art.º 2º)

É introduzida uma menção nova, face à 1 ª versão, segundo a qual os operadores devem cumprir as suas obrigações em matéria de segurança e integridade de redes e serviços tendo em conta aspetos climatéricos e riscos de desastres naturais e fenómenos extremos, e atendendo a informação prestada por entidades oficiais sobre estes temas, bem como a Estratégia Nacional de Adaptação às Alterações Climáticas 2020.

Sem prejuízo das várias medidas que os operadores já adotam para aumentar a resiliência das suas redes aos aspetos e fenómenos mencionados, tendo em conta as iniciativas que a ANACOM tem promovido sobre estas matérias, entendemos que será sempre útil que haja uma coordenação setorial das medidas a adotar, tendo em devida conta os contributos dos operadores. Por outro lado, o setor beneficiará do estabelecimento de canais de informação formais com as diversas entidades e autoridades que intervêm nestas matérias (ex.: ANPC, IPMA, ICNF) e da disponibilização da informação em formatos digitais integráveis e tratáveis pelos sistemas operacionais dos operadores.

3.2. Meios eletrónicos (Art.º 5º)

Como já referido nos comentários genéricos, consideramos que deve ser minimizada a troca de informação sensível sobre segurança e integridade das redes e serviços entre os operadores e a ANACOM, mesmo que tal seja feito via um sistema de informação específico. Por outro lado, a informação a trocar deve apenas ser aquela necessária para que o Regulador garanta a execução das funções que lhe estão atribuídas legalmente.

Assim, consideramos que a informação a enviar à ANACOM pelos operadores não deverá incluir informação cadastral, nomeadamente sobre ativos críticos de rede, devendo limitar-se às notificações sobre incidentes de segurança, documentação de auditorias e relatório anual de segurança.

Por outro lado, enquanto o sistema de informação mencionado no artigo não estiver disponível, existe um risco acrescido de interceção de informação sensível caso se troque essa informação por meios não seguros, tais como correio normal ou correio eletrónico, o que mais aconselha à minimização das trocas de informação sensível.

Em qualquer caso, a ANACOM poderá sempre consultar os sistemas e registos dos operadores, por meio da deslocação de colaboradores seus devidamente credenciados, às instalações dos operadores.

3.3. Medidas técnicas de execução e requisitos adicionais (Art.º 7º)

A 2ª versão do Regulamento determina que os operadores devem adotar todas as medidas de segurança incluídas nos níveis de sofisticação 1 e 2 para prossecução de cada um dos 25 OS listados no Anexo.

São admitidas as seguintes exceções justificadas por análise de riscos:

- Não adoção de uma ou todas as medidas de nível 2 para um objetivo, mediante autorização prévia da ANACOM
- Adoção de uma ou todas as medidas de nível 3 para um objetivo, não sendo necessária autorização prévia da ANACOM

As seguintes 11 medidas específicas são obrigatórias:

- Classificação de ativos e elaboração do inventário de ativos (artigos 8º e 9º)
- Requisitos de gestão de riscos (artigo 10º)
- Procedimentos de controlo da gestão excecional de tráfego de acesso à Internet (artigo 11º)
- Exercícios (artigo 12º)
- Informação aos clientes (artigo 13º)
- Responsável de segurança (artigo 14º)
- Ponto de contacto permanente (artigo 15º)
- Equipa de resposta a incidentes de segurança (artigo 16º)
- Plano de segurança (artigo 17º)
- Deveres de comunicação à ANACOM (artigo 18º)
- Relatório anual de segurança (artigo 19º)

Como já referido, embora se saúde a adoção de um nível de sofisticação menos elevado do que na 1ª versão do Regulamento e algum grau de flexibilidade previsto nas alíneas a) e b) do nº 1 deste artigo, mesmo assim, a adoção do nível 2 para todas as medidas técnicas de execução de todos os OS parece-nos excessiva, tendo em conta os níveis de risco a que os operadores nacionais estão expostos. Por outro lado, não foi feita uma análise de risco nem de custo-benefício que justifique a adoção deste nível em termos globais. Note-se que um operador pode já ter adotado diferentes níveis de sofisticação para os diferentes OS, em função de análises de risco já realizadas, estando já adequadamente adaptado ao nível de risco que enfrenta.

Face à nossa experiência, considerando os impactos operacionais e de investimento, entendemos que seria mais razoável a adoção do nível 1 como base e a definição de um prazo de evolução para níveis de sofisticação mais elevados, tendo em conta análises de risco que o justificassem. Em alternativa, consideramos que seria razoável adotar o nível 1 como base e estabelecer como objetivo atingir-se, num processo de melhoria contínua a realizar num prazo razoável, 80% das medidas estabelecidas no Anexo do Regulamento. Assim, sugere-se que se altere o art.º 7 num destes sentidos, bem como os prazos relevantes previstos no art.º 35º.

3.4. Classificação de ativos (Art.º 8º)

É definida uma classe A, que combina as classes A e B da 1ª versão do Regulamento, sendo introduzida alguma simplificação nas definições. No entanto, em termos práticos, não haverá grande simplificação na classificação de ativos para os principais operadores nacionais, que continuarão a ter de classificar vários dos seus ativos nesta classe. A este propósito, a alínea d) do nº 3 refere como classificáveis na Classe A ativos que assegurem *"[…] interligação entre as Regiões Autónomas, interligação entre o Continente e uma Região Autónoma ou interligação entre ilhas na Região Autónoma dos Açores ou na Região Autónoma da Madeira […]"*. Consideramos esta exigência excessiva para operadores com um pequeno número de clientes nas Regiões Autónomas, pelo que sugerimos que só sejam classificáveis na Classe A ativos nas condições da alínea d) do nº 3 que também sirvam pelo menos 1.000 assinantes ou acessos (o limite inferior de assinantes/acessos passível de motivar uma notificação ao Regulador).

Assinala-se, por outro lado, que as alíneas c) e e) do nº 3 deste artigo introduzem uma indeterminação significativa na classificação de ativos, pois, por um lado, a ANACOM poderá, a todo o momento, com um pré-aviso de cinco dias úteis, designar entidades adicionais no âmbito da alínea f) do nº 2 do art.º 21º ("clientes críticos"), e, por outro lado, ainda não foram comunicados os ativos que se integram na alínea e).

É definida uma classe B de ativos, que não estejam incluídos na Classe A, mas cuja afetação cause *"um impacto negativo grave na segurança das redes e serviços ou na sua continuidade"*. Considera-se a definição demasiado vaga e sujeita a múltiplas interpretações. Entendemos que nesta classe deviam ser incluídos os ativos considerados críticos pelos operadores e que não estejam já classificados como ativos de classe A, pelo que se sugere a revisão da definição da classe B neste sentido.

3.5. Inventário de ativos (Art.º 9º)

O inventário passa a incluir todos os ativos (anteriormente não incluía ativos não críticos, correspondentes à atual classe C). No entanto, só para os ativos críticos (novas classes A e B) é exigida informação detalhada.

Mesmo assim, a informação a fornecer para todos os ativos é a seguinte:

- Identificador único
- Designação
- Classificação (Classe A, B ou C)
- Coordenadas geográficas da sua localização
- Identificação das entidades detentoras ou gestoras do local

Para os ativos críticos (classes A e B) é exigida a seguinte informação adicional:

- Funcionalidades e serviços suportados
- Fundamentação da classificação, incluindo descrição do impacto potencial de uma perturbação de funcionamento, incluindo em termos de redundância, robustez e resiliência
- Identificação como ponto de falha única
- Fornecimentos de terceiros críticos para o seu funcionamento (ex.: serviços de gestão, de operação, de segurança, de energia)
- Autonomia em caso de falha de energia
- No caso de interligação, identificação do tipo e das empresas interligadas
- Medidas, controlos e registos de segurança adotados
- Registo de incidentes de segurança significativos ocorridos
- Registo de alterações efetuadas, incluindo resultados de testes de integração e de sistema realizados e os planos de restauro dos ativos

Os operadores com ativos da Classe A devem comunicar à ANACOM uma lista com os ativos das Classes A e B com a informação geral aplicável a todos os ativos e com a justificação da classificação e descrição do impacto de uma potencial perturbação de funcionamento.

Estas disposições apresentam vários problemas, que abaixo se enumeram e analisam.

Em primeiro lugar, é exigido um conjunto de informação comum sensível, tal como coordenadas geográficas e entidades detentoras ou gestoras do local, mesmo para ativos de classe C, não críticos.

Consideramos que os ativos de classe C devem ser excluídos do cadastro.

Por outro lado, para os ativos de classe A e B deve ser enviada à ANACOM a informação relativa a coordenadas geográficas e entidades detentoras ou gestoras do local, bem como a justificação da classificação e descrição do impacto de uma potencial perturbação de funcionamento. Esta informação é extremamente sensível e a sua transmissão constitui um potencial risco de segurança, pelo que discordamos do seu envio nos termos descritos. Sem prejuízo, a ANACOM poderá sempre ter acesso a tal informação diretamente nas instalações do operador, como já defendido em ponto anterior.

3.6. Requisitos de gestão de riscos (Art.º 10º)

Todas as exigências constantes da 1ª versão do Regulamento relacionadas com gestão de riscos são eliminadas e substituídas por uma exigência de revisão, a cada dois anos, da metodologia de gestão de riscos e das ferramentas adotadas pelos operadores.

Saúda-se e eliminação das anteriores disposições sobre gestão de riscos mas considera-se que não faz sentido definir-se uma exigência de revisão da metodologia de gestão de riscos. Esta metodologia constitui a base de toda a análise de riscos. O que faz sentido e se aceita é proceder à revisão periódica da análise de riscos, de forma a determinar a adequação das medidas técnicas de execução implementadas face ao cenário de risco que o operador enfrenta. Assim, sugere-se a revisão do artigo segundo este entendimento.

3.7. Exercícios (Art.º 12º)

São simplificadas as disposições da 1ª versão do Regulamento relativas aos exercícios, o que se saúda. A periodicidade passa a ser no máximo bianual. Entende-se que se pretendia definir uma periodicidade máxima de dois anos, pelo que se sugere que o termo bianual, que também significa "duas vezes por ano", seja substituído explicitamente por essa indicação.

Mesmo assim, considera-se que uma periodicidade de dois anos nos exercícios poderá ser excessiva, pelo que se sugere o alargamento para três anos.

Em qualquer caso, assinala-se que a realização de exercícios envolvendo ativos de classe A e B acarretam um risco elevado, pelo que se sugere que estes possam ser excluídos em alguns casos. Por exemplo se houver redundância para tais ativos ou se estiverem abrangidos pelo plano de continuidade de negócio, consideramos que poderiam ser excluídos dos exercícios.

3.8. Informação aos clientes (Art.º 13º)

Os operadores têm de informar os seus clientes que façam parte da lista de clientes críticos das medidas adotadas na sequência de incidentes de segurança que tenham um impacto negativo na oferta de redes e serviços através dos quais esses clientes prestam os seus serviços relevantes à sociedade.

A ANACOM também deve receber essa informação, sem prejuízo do disposto no Regulamento sobre notificações de incidentes de segurança.

Para além das indeterminações existentes e já assinaladas sobre a lista de clientes críticos, estes clientes, que integrarão seguramente setores de atividade de que os operadores também dependem, como por exemplo o setor energético, passam a ter uma situação de privilégio em relação aos operadores, dado que não existem obrigações equivalentes impostas aos outros setores de atividade em benefício do setor das comunicações eletrónicas. Acresce que os operadores já disponibilizam aos seus clientes mais relevantes a informação que estes contratualmente exigem e que cumpre as suas necessidades de informação relacionadas com incidentes de segurança ou quebras de serviço.

Assim, não se vê qualquer vantagem em manter as exigências deste artigo do Regulamento.

3.9. Ponto de contacto permanente (Art.º 15º)

Uma vez que ainda não é clara a articulação dos operadores com e as suas obrigações no âmbito do planeamento civil de emergência e do plano de emergência de proteção civil, reiteram-se as solicitações já feitas ao Regulador pelo setor das comunicações eletrónicas para que proceda à clarificação destes aspetos. Em qualquer caso, deve ser deixado ao critério dos operadores a adequação da sua estrutura operacional às exigências que forem determinadas.

3.10. Equipa de resposta a incidentes de segurança (Art.º 16º)

A 1ª versão do Regulamento foi totalmente alterada neste aspeto. Anteriormente todos os operadores eram obrigados a constituir equipa de resposta a incidentes de segurança, para lidar com incidentes que afetassem ativos das anteriores classes A, B, C ou outros ativos críticos.

Na nova versão apenas operadores com ativos da nova classe A devem dispor desta equipa, para lidar com incidentes que afetem ativos das novas classes A ou B. A equipa também deverá integrar o sistema de resposta a incidentes de segurança da informação, em termos a determinar ao abrigo da Lei das Comunicações Eletrónicas.

Como já referido, embora haja uma simplificação das exigências nesta matéria, espera-se que, na prática, todos os principais operadores nacionais venham a ter de constituir estas equipas, dado que todos deverão ter ativos de classe A. Assim, torna-se crítico que o Regulador defina a forma como estas equipas irão integrar o sistema de resposta a incidentes de segurança da informação e como será coordenada a atuação do setor das comunicações eletrónicas com a Estrutura de Segurança do Ciberespaço prevista na Lei nº 46/2018, de 13 de agosto.

3.11. Relatório anual de segurança (Art.º 19º)

Consideramos que a inclusão, por via da alínea b) do nº 1 deste artigo, das estatísticas trimestrais de todos os incidentes de segurança, incluindo os sem impacto significativo, é excessiva e injustificável. Os incidentes sem impacto significativo não deverão fazer parte do relatório.

3.12. Formato e procedimentos das notificações à ANACOM (Art.º 22º)

A notificação de fim de impacto significativo deve passar a incluir informação adicional, face ao regime atual, nomeadamente indicando as freguesias (atualmente identificam-se os concelhos) onde houve assinantes ou área geográfica afetada.

Alerta-se que passar a disponibilizar a informação relativa a freguesias afetadas introduz um nível de complexidade significativo no processo de notificação, uma vez que a estrutura das redes não está diretamente mapeada em divisões administrativas e, por outro lado, a localização dos impactos dos incidentes não é fácil de determinar, com essa granularidade geográfica, no momento da notificação de fim de impacto significativo. Também não se vê vantagem, do ponto de vista da gestão e resolução do incidente, em prestar informação de localização a nível da freguesia.

Assim, defendemos que deve manter-se o atual regime de informação geográfica ao nível do concelho. Sem conceder, caso o Regulador insista em receber informação a nível de freguesias afetadas, entendemos que tal informação só poderá ser fornecida, com impacto mínimo a nível processual e de desenvolvimento de sistemas, na notificação final.

3.13. Conteúdo, meios e prazos de divulgação ao público (Art.º 23º)

O Regulamento determina que a informação divulgada ao público deve passar a incluir a indicação da zona ou das zonas afetadas, desagregada ao nível da freguesia, se possível de modo gráfico sobre um mapa de Portugal.

Não vemos vantagem para o cliente final em disponibilizar a informação com esta granularidade geográfica e com este formato visual. Acresce que as dificuldades assinaladas a propósito das notificações à ANACOM, relacionadas com a identificação de localização de área afetada ao nível da freguesia, se mantêm, obviamente, na informação a divulgar ao público, pelo que será, em geral, muito difícil ter tal informação disponível. Independentemente disso, a disponibilização em formato de mapa implica desenvolvimentos e investimentos em sistemas que não contribuem para uma resolução mais rápida dos incidentes, não se traduzindo em qualquer benefício prático para o que realmente interessa ao cliente final, que é reposição dos serviços afetados.

O Regulamento também impõe que a informação ao público deve ser disponibilizada no prazo máximo de uma hora após notificação inicial à ANACOM e que deve ser permanentemente atualizada.

Como já referido, a informação sobre incidentes que é disponibilizada ao público é sempre preparada pela área de Comunicação / *Public Relations* do operador, tendo em conta a informação disponibilizada pelas áreas técnicas, uma vez que a linguagem usada tem de ser adequada à comunicação com o público e seguir as linhas de orientação de comunicação e imagem da empresa. As equipas de comunicação não estão disponíveis 24 horas por dia e sete dias por semana como as equipas de intervenção técnica. Assim, é impossível assegurarem, permanentemente, a divulgação ao público de informação sobre incidentes uma hora após notificação inicial à ANACOM e com garantia de permanente atualização. O cumprimento estrito do que está disposto no Regulamento implicaria a criação de equipas de comunicação disponíveis em permanência, à semelhança das equipas técnicas de resolução de incidentes, o que é totalmente desproporcional e injustificável.

Assim, entendemos que o Regulamento deverá manter o regime em vigor de comunicação ao público de incidentes de segurança com impacto significativo.

3.14. Auditoras (Art.º 28º)

O nº 3 do artigo determina que os operadores devem assegurar a rotatividade na escolha de auditoras, de modo a que a mesma auditora não realize mais do que duas auditorias consecutivas. Consideramos esta exigência excessiva uma vez que bastará assegurar que as equipas auditoras sejam sujeitas a rotatividade, mesmo que pertençam à mesma empresa auditora. Aliás, isto já é assegurado pelas empresas auditoras.

Assim, sugere-se que o referido número seja alterado para determinar a rotatividade das equipas auditoras e não das empresas auditoras, sendo aceitável o limite indicado de duas auditorias consecutivas.

3.15. Fases de auditoria (Art.º 31º-33º)

Mantêm-se as fases de auditoria previstas na 1ª versão, bem como a informação a enviar à ANACOM, mas alteram-se alguns prazos.

Consideramos que o processo é excessivamente burocrático.

Assim, na fase de pré-auditoria o operador deverá estar simplesmente obrigado a enviar à ANACOM o plano de auditoria, para que a ANACOM, querendo, possa acompanhar a auditoria, não devendo este programa estar dependente de aceitação pelo Regulador. Aceitam-se os prazos indicados no Regulamento para esta fase.

Nestas condições, a auditoria realiza-se na data e locais previstos no programa. Caso a ANACOM entenda acompanhar a auditoria, deverá indicar ao operador, com uma antecedência adequada, qual o seu colaborador que acompanhará os trabalhos. Este colaborador deverá, no nosso entendimento, por questões de equidade, cumprir todos os requisitos exigidos aos auditores, ou seja, todo o nº 1 do art.º 28º e não apenas a alínea c) deste nº.

3.16. Entrada em vigor e disposições transitórias (Art.º 35º)

Não se compreende a redução de 18 meses, prevista na 1ª versão do Regulamento, para 80 dias úteis, prevista na 2ª versão, do prazo de implementação dos procedimentos de controlo de gestão excecional de tráfego de acesso à Internet a que alude o art.º 11º. Com efeito, tais procedimentos exigirão desenvolvimentos por parte dos fornecedores, o que não está sob controlo dos operadores. Assim, solicita-se a manutenção do prazo de 18 meses previsto na 1ª versão do Regulamento.

Sem prejuízo do que defendemos sobre a adoção do nível de sofisticação 1 para as medidas técnicas de execução de todos os OS previstos no Anexo ao Regulamento, entendemos que o prazo de 18 meses definido para o ponto *ii)* da alínea d) do nº 2 do art.º 35º, para a adoção de "*todas as restantes medidas de segurança aplicáveis nos termos do previsto no Título II e no Anexo ao presente regulamento, sem prejuízo do disposto nos nº 3 e 5 do presente artigo"* deve ser alargado para 36 meses, de forma a diluir no tempo o impacto operacional e financeiro expectável.