RELATÓRIO DA AUDIÊNCIA PRÉVIA E DO PROCEDIMENTO GERAL DE CONSULTA SOBRE O SENTIDO PROVÁVEL DE DECISÃO RELATIVO:

- **Às circunstâncias, ao formato e aos procedimentos aplicáveis às exigências de comunicação das violações de segurança ou das perdas de integridade com impacte significativo no funcionamento das redes e serviços, pelas empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público (N.º 2 do artigo 54.º-C e artigo 54.º-B, ambos da LCE);**
- **Às condições em que o ICP-ANACOM considera existir um interesse público na divulgação ao público, por parte das empresas que oferecem redes de comunicações públicas ou serviços de comunicações electrónicas acessíveis ao público, das violações de segurança ou das perdas de integridade com impacte significativo no funcionamento das redes e serviços (alínea b) do artigo 54.º-E da LCE).**

A - ENQUADRAMENTO

O ICP – Autoridade Nacional de Comunicações (ICP-ANACOM) aprovou em 22 de Dezembro de 2011, por deliberação do seu Conselho de Administração, o sentido provável de decisão ("SPD" no presente documento), relativo:

- Às circunstâncias, ao formato e aos procedimentos aplicáveis às exigências de comunicação das violações de segurança ou das perdas de integridade com impacte significativo no funcionamento das redes e serviços, pelas empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público (N.º 2 do artigo 54.º-C e artigo 54.º-B, ambos da LCE);

- Às condições em que o ICP-ANACOM considera existir um interesse público na divulgação ao público, por parte das empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público, das violações de segurança ou das perdas de integridade com impacte significativo no funcionamento das redes e serviços (alínea b) do artigo 54.º-E da LCE).

Foi ainda decidido submeter este projeto de decisão a audiência prévia das entidades interessadas, nos termos dos artigos 100.º e 101.º do Código de Procedimento Administrativo, bem como ao procedimento geral de consulta, previsto no artigo 8.º e no n.º 4 do artigo 54.º-C da Lei das Comunicações Eletrónicas ("*LCE*" no presente documento, aprovada pela Lei n.º 5/2004, de 10 de fevereiro, sucessivamente alterada pelo Decreto-Lei n.º 176/2007, de 8 de maio, pela Lei n.º 35/2008, de 28 de julho, pelo Decreto-Lei n.º 123/2009, de 21 de maio, pelo Decreto-Lei n.º 258/2009, de 25 de setembro, pela Lei n.º 51/2011, de 13 de setembro, pela Lei n.º 10/2013, de 28 de janeiro e pela Lei n.º 42/2013, de 3 de julho), fixando-se em ambos os casos o prazo de 20 dias úteis para os interessados se pronunciarem, prazo esse que terminou a 27 de Janeiro de 2012.

No âmbito deste procedimento, foram recebidos, dentro de prazo, os contributos de:

- empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público (*"empresas"* no presente documento), a saber AT&T/COLT/Verizon Business em manifestação conjunta, Cabovisão, CTT, Grupo ONI (Onitelecom, Knewon, e F300), Optimus, Grupo PT (Portugal Telecom, S.G.P.S., S.A., PT Comunicações, S.A., e TMN – Telecomunicações Móveis Nacionais, S.A.), Vodafone e ZON (ZON TV CABO, ZON TV CABO MADEIRENSE e ZON TV CABO AÇOREANA), assim como da Associação dos Operadores de Telecomunicações (APRITEL);
- associações de defesa dos consumidores, a saber a Associação de Consumidores de Portugal (ACOP) e a União Geral de Consumidores (UGC); e
- entidades públicas, a saber a Direção Geral do Consumidor (DGC) e a Secretaria Regional da Educação e Recursos Humanos do Governo Regional da Madeira (GRM).

Fora de prazo, foram ainda recebidos o contributo da Associação Portuguesa para a Defesa do Consumidor (DECO) e uma versão revista do contributo da Optimus, os quais, por essa razão, não foram considerados no presente relatório.

Concluído o processo de consulta, importa agora elaborar o relatório daí resultante e proceder à divulgação pública das respostas recebidas, expurgadas dos elementos considerados confidenciais, as quais foram tidas em conta em toda a sua extensão e não apenas relativamente ao conteúdo transposto ou referido na síntese incluída no presente relatório.

O presente relatório apresenta assim a síntese das respostas recebidas na consulta pública e o entendimento do ICP-ANACOM sobre a matéria, fundamentando as opções tomadas na decisão final.

Antes de mais, porém, e no que respeita à sugestão do Grupo PT para a *"constituição de um Grupo de Trabalho integrando todos os interessados, de forma a garantir quer a definição de incidentes de segurança a reportar, quer a definição de medidas proporcionais adequadas à realidade prática do setor e que tomem em consideração a criticidade dos serviços"*, adianta-se, desde já, ser entendimento do ICP-ANACOM que, no atual enquadramento, não pode tal sugestão ser acolhida, sendo certo que:

a) Nos termos do n.º 2 do artigo 54.º-C da LCE, compete ao ICP-ANACOM aprovar as medidas que definam as circunstâncias, o formato e os procedimentos aplicáveis às exigências de comunicação de violações de segurança ou perdas de integridade das redes; e

b) Nos termos do n.º 4 do mesmo artigo, a adoção destas medidas de execução está sujeita ao procedimento geral de consulta previsto no artigo 8.º da LCE, pressupondo assim a lei ser esta a via adequada para incorporar os contributos dos interessados com vista ao aperfeiçoamento desta decisão.

Em qualquer caso e após a entrada em vigor desta decisão, encontrar-se-á esta Autoridade sempre disponível para a receção e análise de quaisquer contributos que possam conduzir a uma eficiente aplicação da mesma.

Por último, importa ainda referir que, após a consulta pública, obteve esta Autoridade conhecimento de estatísticas relativas às ocorrências de crimes de furto e de danos em infraestruturas utilizadas para a disponibilização de redes e serviços de comunicações eletrónicas nos anos de 2010 e 2011.

Tendo procedido à análise dos factos com vista a averiguar da sua relevância para o processo decisório em curso concluiu o ICP-ANACOM, no entanto, que dos mesmos não resultaram novos elementos relevantes para a presente decisão.

B - CONSIDERAÇÕES GERAIS

1. Por parte das empresas e da APRITEL:

- **AT&T, COLT e Verizon Business**, em resposta conjunta na língua inglesa[1], referem a sua especificidade enquanto empresas limitadas apenas ao fornecimento de serviços pan-europeus e globais a grandes clientes empresariais, relevando enquanto tal a necessidade de uma implementação totalmente idêntica em todos os Estados-Membros da União Europeia (UE), em nome dos benefícios que advêm duma aproximação coordenada em toda a UE, desejavelmente atingível mesmo que sem medidas formais de harmonização.

  Em linha com o referido consideram aquelas empresas que o ICP-ANACOM devia alinhar pelo documento[2] publicado pela ENISA[3] em 10.12.2011, concedendo embora que o relatório das empresas às Autoridades Reguladoras Nacionais (ARN) está fora do âmbito daquele documento.
- A **Cabovisão** *"saúda a iniciativa do ICP-ANACOM de definir as circunstâncias, formato e procedimentos aplicáveis à exigência de comunicação de violações de segurança e integridade de redes, (…) considerando que só assim se garante a coerência na abordagem à matéria (…)"*.

  Refere ainda que *"confere uma importância primordial à proteção da integridade e segurança das redes e serviços de comunicações eletrónicas, visível nos avultados investimentos que tem feito nesta matéria (…)"*.

  Entende no entanto a Cabovisão, sem prejuízo do exposto, *"que é fundamental que o ICP-ANACOM revisite determinados aspetos contemplados no Projeto de Decisão relativo à comunicação de incidentes de segurança (Projeto de Decisão I), sob pena de adotar uma posição demasiado exigente, sem paralelo nas posições assumidas pela ENISA e pela OFCOM (…)"*.
- Os **CTT** referem que, na sua qualidade de operador móvel virtual, *"prestam todos os seus serviços de comunicações eletrónicas suportados na rede móvel*

[1] Razão pela qual se salvaguarda, em todo o presente documento, eventuais desvios que surjam na nossa tradução e respetivo entendimento, relativamente ao que alegadamente pretenderiam aquelas empresas ao expressarem-se na língua inglesa.
[2] Disponível em http://www.enisa.europa.eu/act/res/reporting-incidents/incidents-reporting-to-enisa/technical-guideline-on-incident-reporting .
[3] *European Network and Information Security Agency*.

da TMN, sendo este operador a entidade responsável pela segurança e integridade dos serviços prestados pelos CTT aos seus clientes" e que, por o SPD fazer *"recair sobre os prestadores como os CTT, operadores sem infraestrutura de rede, as obrigações de segurança e integridade da rede onde são suportados os seus serviços"*, terão de ser subcontratados novos serviços no âmbito do contrato celebrado com a TMN para dar cumprimento às obrigações agora estabelecidas.

Entendem ainda *"que face à pequena dimensão dos CTT (…), o cumprimento de obrigações em matéria de segurança de redes implicará um custo administrativo significativo na sua atividade, tendo um impacto direto nos consumidores finais, seus clientes"*, motivo de grande preocupação para os CTT, pelo que *"deverá o ICP-ANACOM estabelecer mecanismos que reflitam a realidade dos operadores não detentores de rede (…), fazendo recair apenas sobre os operadores detentores de rede as obrigações agora sujeitas a consulta, já que apenas estes terão os meios para detetar e identificar incidentes de segurança na sua rede"*.

- O **Grupo ONI** considera que o SPD representa *"um passo importante para a implementação operacional das disposições já transpostas para a Lei Nacional, pelo que se saúda esta iniciativa do ICP-ANACOM. No entanto, as disposições constantes do SPD carecem de ajustes importantes para estarem alinhadas com a realidade do mercado, terem em conta a real utilidade da informação a prestar, não contribuir para um aumento do nível de risco e não causar alarmismos injustificados no público, nem contribuir, indevidamente, para a má imagem do sector."*.
- A **Optimus** partilha com o ICP-ANACOM a relevância atribuída à segurança e integridade das redes e serviços, tendo por isso *"implementados diversos procedimentos internos de garantia e prevenção de incidentes de segurança, nomeadamente, relacionados com a interrupção de serviço (…) consubstanciados em diversas vertentes."*.

  Alega que, na sua opinião, as determinações do SPD relativas às *"(exigentes) obrigações de notificação propostas"* não preenchem os requisitos definidos no artigo 5.º da LCE, e a serem adotados os parâmetros ali presentes *"o ICP-ANACOM poderia receber uma quantidade elevada de notificações dos operadores que decorrem naturalmente das incidências da atividade de gestão de uma rede que está sujeita a falhas de equipamentos e serviços, mas que*

não são verdadeiramente significativas do ponto de vista nacional, nem para o público:".

A Optimus refere também a necessidade de se clarificar o tipo de intervenção do ICP-ANACOM durante um incidente de segurança face aos prazos de notificação.

Acrescenta ainda que *"O âmbito dos serviços e os parâmetros a considerar para notificação deverão refletir circunstâncias de falha que são realmente fundamentais e críticas e que afetem a segurança nacional ou representem situações de emergência"*, e salienta *"que o ICP-ANACOM na avaliação da proporcionalidade e razoabilidade das medidas a impor não poderá deixar de ponderar os custos de implementação e de operação. As obrigações que venham a ser definidas não podem implicar a realização de investimentos avultados, nem um acréscimo considerável dos custos administrativos para os operadores, sem que sejam claros os seus benefícios para o mercado, em geral, e para os utilizadores, em particular. Este aspecto é particularmente relevante no atual contexto macroeconómico e financeiro caracterizado pela queda da atividade económica e dificuldades de acesso a financiamento."*.

- O **Grupo PT** releva o caráter "*ex novo"* da matéria em apreço, e a importância que atribui à segurança e que levou à realização de investimentos consideráveis nesta área e à criação de um Comité de Segurança e de um Comité de Privacidade e de Proteção de Dados Pessoais.

  Pela importância que dão a todas as questões relacionadas com a Segurança e Integridade de Redes e Serviços *"é com agrado que assistimos à consagração, ao nível legal e regulamentar, de medidas que, certamente, contribuirão para reforçar o enfoque dos operadores na adoção de medidas tendentes a assegurar um risco mínimo em termos de segurança e de integridade das respetivas redes. Adicionalmente, não devem ser relegados para segundo plano os claros benefícios que tal atuação terá para o sector, globalmente considerado, porquanto aportará claros benefícios para todos os stakeholders."*.

  Expressam no entanto o seu não acordo com alguns aspetos do SPD, como o estabelecimento de *"condições (triggering thresholds) mais exigentes que os estabelecidos, por exemplo, pelo OFCOM, quer no que respeita à duração do incidente a considerar para efeitos de notificação, quer quanto aos próprios prazos de notificação, e bem assim quanto ao número de notificações que poderão ocorrer e respetivo conteúdo, entre outros aspetos."*, e a necessidade

de se *"recorrer ao benchmark existente e à ratio inerente à obrigação de notificação – garantir que apenas os incidentes realmente significativos sejam notificados – para avaliar os reais benefícios que poderão advir das notificações"*.

Referem que previamente à definição dos procedimentos de notificação, deveriam ser concretizadas as medidas técnicas consideradas adequadas a que se refere o artigo 54.º-A da LCE, e fazem um entendimento em paralelo com o racional da notificação de violação de dados pessoais aos assinantes constante da Diretiva Privacidade.

Referem ainda: a necessidade de uma definição concreta de *"incidente de segurança"*, a eventual desproporção de custos incorridos face aos objetivos que se pretendem atingir (invocando uma vez mais o documento do OFCOM), a necessidade de balizar os serviços abrangidos tendo presente a sua criticidade, *"como o faz por exemplo, a ENISA na sua proposta de template de comunicação"*, e as diferenças que em sua opinião deverão existir entre MNOs e MVNOs.

Consideram que o SPD, em matéria de notificação ao ICP-ANACOM, *"implica um esquema de reporte excessivamente burocrático, que deverá ser flexibilizado e aligeirado"*.

Relativamente à informação aos utilizadores, alertam para o *"aproveitamento que um incidente de segurança pode ter pelos media, sobretudo aqueles que têm uma linha editorial mais sensacionalista"*, e lembram que a avaliação do interesse público na divulgação de incidentes de segurança é uma obrigação do ICP-ANACOM tal como a lei prevê, defendendo que essa divulgação deverá ser feita numa base casuística.

Por último manifestam a sua discordância quanto ao prazo de implementação de 30 dias proposto pelo ICP-ANACOM, e sugerem a criação de um Grupo de Trabalho integrando todos os interessados, para o qual manifestam a sua disponibilidade, com base no seu entendimento de que qualquer decisão adotada pelo Regulador relativamente à matéria em apreço deveria resultar dos esforços de coordenação entre o ICP-ANACOM e as empresas de redes e serviços de comunicações eletrónicas.

- *"A **Vodafone** está ciente da importância em assegurar a contínua segurança e integridade das redes e serviços de comunicações eletrónicas, (…) tendo, naturalmente, implementado os necessários mecanismos de prevenção e gestão dos riscos decorrentes de eventuais incidentes de segurança."*.

Considera a Vodafone que, no SPD, vem o ICP-ANACOM utilizar critérios não alinhados com os utilizados pela ENISA, como sejam a notificação de incidentes cuja duração seja inferior a uma (1) hora, para além de impor *"um conjunto de critérios adicionais, igualmente não previstos nas orientações da ENISA, e prazos imperativos de notificação dos incidentes manifestamente exíguos, o que torna o procedimento de notificação mais complexo e exigente, quer do ponto de vista técnico, quer administrativo e, por conseguinte, mais oneroso para os operadores."*.

"Deste modo, se atendermos ao desvio evidente que é feito pelo ICP-ANACOM, sem justificação para tal, na delimitação do tipo de incidentes a reportar face aos critérios definidos a nível europeu, ao racional subjacente às obrigações de notificação, bem como aos encargos que tal abordagem comporta para os operadores, não podemos deixar de concluir que as medidas impostas no referido Projeto Decisão são desproporcionais.".

Relativamente ao interesse público na divulgação ao público de um incidente de segurança, entende a Vodafone que a avaliação deve ser casuística e que a utilização de critérios iguais aos utilizados para a notificação ao regulador é desadequada e injustificada; esta posição suscita à Vodafone as maiores reservas devido ao facto de que se poderá concluir que um incidente notificado não teve impacto significativo e portanto a sua divulgação ao público no prazo previsto vir a não se justificar.

Por último, alegando a novidade da matéria e a insuficiência do prazo de implementação de 30 dias previsto no SPD, requerem o estabelecimento de um período não inferior a 6 meses.

- *"A **ZON**, seguindo as melhores práticas do setor, tem investido profundamente em processos de controlo interno visando a garantia e prevenção de incidentes de segurança, bem como participado, aos mais diversos níveis, nos fóruns especializados de acompanhamento e investigação de práticas de políticas de segurança"* e *"está particularmente empenhada na prevenção e combate a violações de segurança e de perdas de integridade que possam impactar as redes e serviços de comunicações eletrónicas"*.

  A ZON entende que o SPD *"apresenta um modelo que significa um conjunto de obrigações que excede largamente o preconizado na Diretiva 2002/21/CE (Diretiva Quadro), alterada pela Diretiva 2009/140/CE, bem como o que a ENISA define na sua Technical Guideline on Incident Reporting",* identificando *"os triggering thresholds preconizados"* com duração mínima muito inferior às

definidas por aquele documento e mesmo quando comparado com as regras de outra ARN (OFCOM), *"os prazos de notificação"* e *"o número de notificações exigidas e respetivo conteúdo (duas notificações obrigatórias e uma terceira eventualmente exigível de acordo com um critério subjetivo)"*.

Quanto à matéria relativa à informação ao público (Anexo B do SPD), a ZON considera que deveria ser definida caso a caso, conforme *"o que resulta do novo n.º 3 do artigo 13.º-A da Diretiva 2002/21/CE, que foi transposto para o Direito Nacional através da LCE"*.

Entende a ZON que deve ser concedido um prazo mínimo de implementação de 6 meses porque *"o presente Projeto de decisão será inovador, não existindo ainda qualquer informação que possa ser obtida de outras NRA sobre as vicissitudes da implementação do referido normativo"*, e conclui que *"as comunicações, ora em análise, não devem impor um novo conjunto de obrigações sem que a respetiva análise de impacto regulatório seja efetuada e partilhada com os stakeholders, servindo a mesma para avaliar os impactos daí resultantes."*.

- A **APRITEL** começa por relevar as referências feitas pelo ICP-ANACOM no SPD quanto à novidade da matéria e quanto ao disposto na LCE ser *"suficientemente preciso para que as empresas possam continuar a desenvolver o seu trabalho."*.

  A APRITEL refere depois que *"os associados da APRITEL já atribuem uma importância primordial à questão da segurança e integridade das suas redes e serviços de comunicações eletrónicas, tendo implementado diversos procedimentos internos de garantia e prevenção de incidentes de segurança e promovido e participado em mecanismos de cooperação setorial, (…) exemplo da prioridade desta matéria para os operadores é o avultado esforço de investimento que o setor, como um todo, realizou na implementação de medidas de garantia de segurança"*.

  Compreendendo o racional do SPD, considera a APRITEL *"que qualquer decisão a tomar neste âmbito, quanto ao tipo de situações que devem ser objeto de notificação, deve pautar-se pela proporcionalidade e flexibilidade de abordagem, tendo em especial conta os encargos que são impostos às empresas (…) e o fim último que se visa assegurar"*, entendendo que o *"ICP-ANACOM acabou por adotar uma posição demasiado exigente para o setor (…) e sem qualquer paralelo nas posições adotadas pela agência ENISA ou por outras entidades reguladoras nacionais, como seja a autoridade Britânica*

OFCOM, (…) isto no que toca quer à duração do incidente, quer aos prazos de notificação, quer ao número de notificações exigidas e respetivo conteúdo, entre outros aspetos".

Reforçam dizendo que, *"na prática, estas exigências correspondem a obrigações que recaem sobre as empresas, implicando custos administrativos significativos, e que são claramente desproporcionais face ao esforço que exigem dos operadores, ao benchmark existente, à ratio da obrigação de notificação – de garantir que apenas os incidentes realmente significativos sejam notificados – à utilidade que o ICP-ANACOM retirará do elevado volume de notificações que expectavelmente receberá caso mantenha os critérios assim definidos e, acima de tudo – sublinhe-se -, às potenciais coimas previstas na LCE para o desrespeito da obrigação de notificação à ARN, que podem ir até €1M"*.

"Já no que respeita ao Projeto de decisão relativo às condições em que o ICP-ANACOM considera existir um interesse público na divulgação ao público, a APRITEL considera desajustada a opção do Regulador em face, por exemplo, da total ausência de orientações da ENISA ou da OFCOM nesta matéria", considerando que o ICP-ANACOM deveria determinar, *"caso a caso, que incidentes merecem divulgação ao público, dadas as respetivas características concretas do caso que determinarão, ou não, a existência de um interesse público na divulgação generalizada ao público"*, como resulta do entendimento que fazem do disposto na LCE (artigo 54.º-E) e na Diretiva 2002/21/CE (n.º 3 do artigo 13.º-A).

A APRITEL não concorda pois com a divulgação ao público *"de todos os incidentes de segurança que são notificáveis ao abrigo do primeiro Projeto de Decisão (Anexo A da consulta)."*, considerando que, *"além de despiciendo e de não ter uma concreta base legal, poderá provocar alarmismo por parte dos consumidores."*.

A APRITEL entende que o ICP-ANACOM deve proceder *"à revisão dos Projetos de Decisão à luz das preocupações do setor no sentido de flexibilizar a sua abordagem e adaptá-la à realidade das empresas, que se descreve nos capítulos seguintes."*.

Por último, a APRITEL expressa *" profunda preocupação dos seus associados quanto ao prazo de implementação definido pelo ICP-ANACOM (…), que deverão dispor de um prazo nunca inferior a 6 meses para implementação dos procedimentos após a divulgação da decisão final."*.

2. Por parte das associações de defesa dos consumidores:

- A **ACOP** manifestou a sua concordância com o proposto.
- A **UGC** emitiu *"parecer favorável ao clausulado proposto por entender que do mesmo até resulta um reforço do direito dos consumidores à informação, designadamente o que resulta do Anexo B."* e considerou *"muito positivo o reconhecimento da necessidade de garantir a segurança e integridade das redes e serviços de comunicações eletrónicas acessíveis ao público tendo em conta a sua importância para todos os cidadãos."*.

3. Por parte da administração pública:

- *"A **DGC** considera esta iniciativa muito importante para os consumidores, não apenas por exigir um esforço qualitativo aos operadores no investimento em segurança e gestão de riscos, mas igualmente na medida em que cria condições para maior visibilidade das situações de rutura da qualidade do serviço, permitindo assim um novo indicador comparativo: a fiabilidade do prestador do serviço."*, (…) entendendo *"que os projetos de decisão devem ser adotados"*.

  Equaciona *"se terá sido ponderado o efeito que os custos de implementação e de gestão dos sistemas poderão ter no aumento dos preços dos serviços. Por outro lado, os diferentes meios e ambientes tecnológicos (adsl, fibra, cobre, por exemplo) refletem capacidades diferenciadas na atuação e tempo de resolução de problemas, o que não está previsto nos projetos de decisão, nem se encontra referenciado no texto."*.
- O **GRM** *"destaca o facto de serem tidas em conta as realidades geográfica e político-administrativas das regiões autónomas"*, no que respeita à obrigatoriedade de comunicação, objeto do Anexo A ao SPD.

4. Entendimento do ICP-ANACOM

Sem prejuízo das posições que o ICP-ANACOM assume adiante na matéria específica dos Anexos A e B do SPD, não podemos deixar de desde já expressar e relevar o nosso entendimento relativamente a alguns pontos atrás referidos e que, a nosso ver, denotam também o cuidado que esta Autoridade teve na abordagem efetuada no SPD quanto aos princípios a aplicar e ao modo de exercer as suas competências, conforme dispõe o artigo 5.º da LCE:

1) O ICP-ANACOM regista com agrado a importância que as empresas que oferecem redes e serviços de comunicações eletrónicas (empresas) atribuem à questão da segurança e integridade das suas redes e serviços, com expressão efetiva nos investimentos alegadamente já realizados, nomeadamente, na implementação de procedimentos de garantia e prevenção de incidentes de segurança.

   Esta era aliás a expetativa desta Autoridade quanto ao resultado da atividade que desenvolveu no passado e referida no SPD, no sentido de *"promover no setor uma cultura de segurança e ao mesmo tempo de alerta e de mudança de mentalidade, destacando a necessidade de, entre outros, as empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público se dotarem de meios que lhes permitam responder em tempo aos novos desafios com que já hoje se defrontam em matéria de segurança e integridade das redes e serviços"*.

2) No que respeita à posição do Grupo PT relativamente à necessidade de uma prévia definição das medidas técnicas de segurança, ao abrigo do disposto no artigo 54.º-A e no n.º 1 do artigo 54.º-C da LCE e apesar de esta matéria ser relativamente recente, facto relevado nos contributos que nos foram enviados e no ponto anterior, reitera-se que, conforme foi adiantado no SPD, *"o disposto na LCE é claro e preciso para que as empresas e o ICP-ANACOM possam desenvolver o seu trabalho nesta matéria no curto prazo (…)"* (sublinhado nosso).

   Com efeito e ao contrário do que é arguido pelo Grupo PT e num sentido que, no geral, se entende ser consentâneo com os contributos das empresas nesta matéria, defende esta Autoridade que seria prematuro proceder à definição das

medidas técnicas a que se refere o disposto no artigo 54.º-A da LCE, entendendo-se que as empresas estarão melhor posicionadas para, num primeiro momento, avaliarem os riscos relativos às suas redes e serviços.

Neste sentido, aliás, concorre o disposto no n.º 2 do artigo 54.º-C da LCE – *"…a ARN pode aprovar e impor (…) medidas técnicas de execução…"* (sublinhado nosso) – quando comparado com o disposto no n.º 1 do mesmo artigo – *"…compete à ARN aprovar as medidas que definam as circunstâncias, o formato e os procedimentos aplicáveis às exigências de comunicação de violações de segurança ou perdas de integridade das redes"* (sublinhado nosso).

O exercício da competência prevista no n.º 1 do artigo 54.º-C da LCE requer assim, no entender desta Autoridade, um acompanhamento contínuo das violações de segurança ou perdas de integridade notificadas ao ICP-ANACOM e uma avaliação da informação que nesse âmbito lhe seja comunicada, incluindo a descrição das medidas que as empresas tenham implementado, sendo que apenas depois dessa avaliação se encontrará esta Autoridade em condições de ponderar uma eventual imposição de medidas técnicas de execução. Naturalmente, tal não isentará a clara e precisa responsabilidade cometida às empresas pelo disposto no artigo 54.º-A da LCE.

3) A posição do Grupo PT no sentido de que o regime de notificação previsto no artigo 4.º da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de julho de 2002 relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas ("Diretiva Privacidade" no presente documento") estaria, no que respeita à divulgação ao público de violações de segurança ou perdas de integridade, mais em linha com os objetivos finais subjacentes à regulação das matérias de segurança de rede, evitando situações de alarmismo generalizado injustificado, não pode merecer a concordância do ICP-ANACOM.

   Em primeiro lugar, há que atender, desde logo, à inequívoca diferença, assumida na revisão do quadro regulamentar comunitário, entre:

   a) Por um lado, o regime de divulgação ao público de violações de segurança ou perdas de integridade, conforme previsto na parte final do 2.º parágrafo do n.º 3 do artigo 13.º-A da Diretiva 2002/21/CE do Parlamento Europeu e do Conselho, de 7 de Março de 2002, relativa a um quadro regulamentar comum para as redes e serviços de

comunicações eletrónicas ("Diretiva Quadro" no presente documento) e, entre nós, na alínea b) do artigo 54.º-E da LCE; e

b) Por outro lado, o regime de notificação de violação de dados pessoais, conforme previsto no 2.º parágrafo e seguintes do n.º 3 do artigo 4.º da Diretiva Privacidade e, entre nós, nos n.os 2 e seguintes do artigo 3.º-A da Lei n.º 41/2004, de 18 de agosto, alterada e republicada pela Lei n.º 46/2012, de 29 de agosto.

Em segundo lugar atente-se no entendimento que expressamos no ponto 10 mais à frente, relevando-se a igual aproximação do regulador finlandês.

4) A referência pela APRITEL de que o ICP-ANACOM deveria flexibilizar a sua abordagem à presente matéria encontra o eco possível, em nossa opinião, na aproximação efetuada por esta Autoridade.

Com efeito não deixando de atender a uma eventual melhoria futura e contínua fruto da perceção e análise que se vier a verificar no seu desenvolvimento, conforme também já tinha sido referido no SPD, o ICP-ANACOM efetuou alguns ajustes neste documento relativamente ao SPD, atentos os comentários recebidos, o que reflete em nosso entender a flexibilidade da aproximação efetuada.

5) As referências pela maioria das empresas e pela APRITEL quanto à necessidade de harmonização, no mercado europeu, das medidas adotadas pelos vários reguladores, às medidas preconizadas no documento "*Technical Guideline on Reporting Incidents*", publicado pela ENISA – European Network and Information Security Agency, ao *benchmark* com outros reguladores, nomeadamente com o OFCOM[4], e as medidas que preconizam (todas do nosso conhecimento, em tempo, e que mereceram a nossa atenção), merece-nos a seguinte posição:

a) Tendo presente que, nos termos do disposto no n.º 4 do artigo 13.º-A da Diretiva Quadro, *"a Comissão, tendo na melhor conta o parecer da ENISA, pode aprovar medidas técnicas de execução adequadas para harmonizar as medidas referidas nos n.os 1, 2 e 3 (…)"*, salienta-se, antes de mais, que, até ao momento, a Comissão Europeia não

[4] Documento disponível em: http://stakeholders.ofcom.org.uk/binaries/telecoms/policy/security-resilience/guidance.pdf

aprovou quaisquer medidas técnicas de execução nesta matéria, facto este, porém, que não pode eximir as ARN do exercício das suas competências dentro dos respetivos enquadramentos legais nacionais;

b) O referido documento "*Technical Guideline on Reporting Incidents*", patrocinado[5] pela ENISA, que foi tido em consideração em todo este processo, não constitui porém o parecer referido no n.º 4 do artigo 13.º-A da Diretiva Quadro, nem reveste, por si, qualquer caráter vinculativo, para além de que tem um objetivo e um âmbito diferentes, pois não contempla as notificações das empresas às ARN nem, neste momento, todas as redes e serviços de comunicações eletrónicas; e tem antes preocupações ao nível europeu, ou seja, não contempla as diferentes realidades nacionais que cabe a cada ARN analisar tendo em conta a legislação adotada pelo respetivo Estado-Membro.

c) Aliás este aspeto da realidade nacional de cada Estado-Membro parece-nos importante, e julgamos que a posição do OFCOM e o seu documento é disso um bom exemplo.

Com efeito a aproximação do OFCOM é efetuada com base numa realidade muito diferente, nomeadamente, face ao nível industrial do setor naquele país, face aos organismos e mecanismos/acordos existentes ao nível da segurança/emergência, face a códigos de conduta adotados, etc, e que permitiram ao OFCOM indicar, por exemplo, que devem ser reportados incidentes de segurança que as empresas tenham consciência que sejam notícia nos *media*[6], ou prescindir (embora não totalmente e por agora[7]) da notificação do incidente de segurança fora de horas normais de expediente devido à existência do NEAT (*National Emergency Alert for Telecoms*), do qual aliás faz parte; caso semelhante acontece na Suécia com o NTCG (*National Telecommunications Crisis Management Coordination Group*)

[5] Com efeito o documento não consubstancia (como explicitamente afirma) qualquer posição ou parecer da ENISA.

[6] 3.49 *"Any incidents that CPs are aware of being reported in the media (local, national or trade news sources)".*

[7] Para grandes incidentes deixam à consideração a notificação em tempo real (3.43 *"CPs may wish to consider submitting reports in real time"*) e colocam a hipótese de revisão desta orientação (3.*40 "we are not planning to monitor received reports outside of normal office hours, although this will be reviewed if required following the introduction of the reporting arrangements"*).

presidido pela PTS (a ARN daquele país).

Releve-se que relativamente a propostas do OFCOM, que de algum modo acolhemos, como a relativa a incidentes repetidos, as empresas de uma maneira geral manifestaram-se contra.

De referir ainda que o OFCOM teve em conta na definição dos serviços e dos *thresholds,* numa interpretação muita específica, as propostas do CPNI[8] (3.50 *"We have developed a set of service specific reporting thresholds to be used as guidance when considering whether a breach of security or loss of availability has 'had a significant impact on the operation' of a network or service, based on proposals from CPNI"*).

d) Importa ainda conhecer, por exemplo, as aproximações entretanto efetuadas pelos reguladores finlandês (FICORA) e sueco (PTS) à matéria em apreço, desde logo porque são entidades que há muito vêm dedicando vastos recursos humanos e financeiros na área da segurança das comunicações, e disponíveis respetivamente em: http://www.ficora.fi/attachments/englantiav/64u7tHKEx/Viestintavirasto57A2012MEN.pdf e http://www.pts.se/upload/Foreskrifter/Tele/ptsfs-2012_2-avbrott-och-storningar.pdf (apenas em língua sueca), relevando-se desde já a questão da informação a disponibilizar aos utilizadores que consta do documento da FICORA (entrada em vigor a 1 de fevereiro de 2012), e os patamares (*thresholds*) definidos no documento da PTS (entrada em vigor a 1 de abril de 2012).

Registe-se igualmente a aproximação do regulador lituano RRT (www.rrt.lt), disponível em https://www.cert.lt/en/legal_acts.html , diferente das demais.

6) Defendendo a Optimus a necessidade de se clarificar o papel do ICP-ANACOM durante um incidente de segurança face aos prazos de notificação fixados esclarece-se, antes de mais, que entende esta Autoridade ser necessário, para uma cabal prossecução das suas atribuições e um correto exercício das suas competências em matéria de segurança e de integridade, ter acesso a informação que lhe permita um acompanhamento em tempo real das violações de segurança e das perdas de integridade, e não somente a sua posterior análise.

De facto e considerando que:

[8] *Centre for the Protection of National Infrastructure*.

a) Nos termos da alínea a) do artigo 54.º-E da LCE, compete ao ICP-ANACOM informar as autoridades reguladoras competentes dos demais Estados Membros e a ENISA sempre que entenda que a dimensão ou gravidade das violações de segurança ou das perdas de integridade comunicadas nos termos do artigo 54.º-B da LCE o justificam;

b) Nos termos da alínea b) do artigo 54.º-E da LCE, compete ao ICP-ANACOM informar o público pelos meios mais adequados das violações de segurança ou das perdas de integridade quando tal seja considerado por esta Autoridade como de interesse público, sem prejuízo das situações nas quais se determina caber às próprias empresas assegurar tal divulgação;

c) Nos termos do n.º 1 do artigo 54.º-G da LCE o ICP-ANACOM pode, para efeitos do disposto nos artigos 54.º-A e 54.º-B e no âmbito das medidas técnicas de execução e dos requisitos adicionais adotados respetivamente ao abrigo dos artigos 54.º-C e 54.º-D, emitir instruções vinculativas às empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público, incluindo a fixação de prazos de execução;

Entende-se, assim, ser necessário dotar o ICP-ANACOM dos meios necessários a um acompanhamento permanente e em tempo real das violações de segurança ou perdas de integridade (*situation awareness*) com vista a que, sempre que seja o caso, possa esta Autoridade informar oportunamente o público, as autoridades reguladoras nacionais de outros Estados Membros e a ENISA, bem como articular ações de resposta e, sendo o caso, emitir instruções vinculativas.

Neste sentido e em geral, relembra-se, o considerando n.º 44 da Diretiva 2009/140/CE do Parlamento Europeu e do Conselho, de 25 de novembro, estabelece que *"as autoridades reguladoras nacionais deverão, por conseguinte, garantir a manutenção da integridade e da segurança das redes de comunicações públicas"*.

Por último, são ainda relevantes nesta sede as atribuições cometidas ao ICP-ANACOM pelo artigo 2.º-A da LCE em matéria de segurança e de emergência, bem como as que no futuro lhe estarão cometidas em sede de planeamento civil de emergência, mercê da sucessão desta Autoridade nas atribuições e

competências da Comissão de Planeamento de Emergência das Comunicações.

7) Quanto à aplicabilidade desta decisão aos MVNO[9], questão suscitada pelos CTT e pelo Grupo PT face a uma alegada inexistência de infraestrutura de rede num MVNO, esclarece-se que:
   a) Nos termos do artigo 54.º-B da LCE, encontram-se obrigadas a notificar o ICP-ANACOM das violações de segurança ou das perdas de integridade com impacte significativo no funcionamento das redes e serviços as empresas que oferecem (i) redes de comunicações públicas ou (ii) serviços de comunicações eletrónicas acessíveis ao público;
   b) De acordo com o esclarecimento já prestado pelo ICP-ANACOM acerca desta matéria e tendo presente as definições constantes do artigo 3.º da LCE, um MVNO é um prestador de serviços de comunicações eletrónicas, podendo ainda, consoante o modelo de negócio adotado e caso controle elementos do sistema de transmissão e da infraestrutura de rede, oferecer redes de comunicações eletrónicas; e
   c) Nesse contexto e na medida em que ofereça serviços de comunicações eletrónicas acessíveis ao público, um MVNO encontrar-se-á assim obrigado a notificar o ICP-ANACOM das violações de segurança ou das perdas de integridade com impacte significativo no funcionamento dos seus serviços e, sendo também esse o caso, no funcionamento das suas redes de comunicações públicas.
8) A necessidade de ser definido o conceito de *"incidente de segurança"*, alegada pelo Grupo PT e pela Cabovisão, merece-nos os seguintes comentários e entendimento:
   a) Na fixação da obrigação de notificação de incidentes de segurança por parte das empresas às ARN, o 1.º parágrafo do n.º 3 do artigo 13.º-A da Diretiva Quadro e, entre nós, o artigo 54.º-B da LCE adotaram, sem qualquer concretização adicional, o conceito de *"violação de segurança ou perda de integridade"*;
   b) Esta ausência de definição, ao nível dos quadros comunitário e nacional, de violação de segurança ou perda de integridade não é, no nosso entendimento, resultado de um qualquer esquecimento mas perfeitamente intencional pois que uma das razões, se não mesmo a

[9] *Mobile Virtual Network Operator* – Operador de Rede Móvel Virtual.

principal, porque esta matéria da segurança e integridade das redes e serviços é trazida para a política regulatória é, nomeadamente, a necessidade de que as Autoridades Reguladoras venham efetivamente a conhecer quais as causas que originam perturbações graves no funcionamento dos serviços prestados pelas redes e serviços de comunicações eletrónicas, a par do reconhecimento de que o conhecimento dessas causas tem, até ao momento, ficado no interior das empresas;

c) A solução adotada, ao nível dos documentos da ENISA e do OFCOM é, por um lado, reconhecer este desconhecimento e, por outro, tentar aproximar as noções de *"violação de segurança ou perda de integridade"* por uma outra que possa conter ambas e que se optou designar *por "incidente de segurança"*;

d) Não importa muito que a definição de incidente de segurança não corresponda a um conceito preciso e fechado, pois o que importa é que tendo-se determinado que um evento, seja ele qual for, provocou a ocorrência de uma perturbação grave no funcionamento das redes e serviços, com impacte significativo na continuidade desse funcionamento, nos termos previstos no n.º 2 do Ponto I do Anexo A e de acordo com as circunstâncias e as regras previstas nos n.os 3 e seguintes do mesmo Ponto I, seja esse evento notificado e, sendo o caso, divulgado ao público;

e) A utilidade da notificação é retirada não só no momento ao informar-se a ARN, mas também posteriormente ao analisar-se quais as causas que a determinaram e quais as medidas tomadas. Assim sendo estamos perante um regime que pretende, por um lado, aumentar a transparência do que se passa na rede ou serviço e, por outro, introduzir um sistema de melhoria contínua na segurança e integridade das redes e serviços de comunicações eletrónicas;

f) Quanto aos documentos da ENISA e do OFCOM, usam conceitos com caráter de orientação técnica não formal, a primeira, e de orientação e de interpretação, a segunda;

g) Releve-se que, nos seus regulamentos, nem a FICORA nem a PTS definiram tais conceitos;

h) Neste sentido e de forma a assegurar uma maior clareza, optou-se por

retirar o termo agregador «incidente de segurança» da versão final da decisão e por adotar a definição adotada, e não concretizada, pelo artigo 54.º-B da LCE: «violação de segurança ou perda de integridade».

9) A maioria das empresas defendeu a necessidade de se definir o âmbito das redes e dos serviços abrangidos com base na sua criticidade, tendo algumas das empresas invocado, para o efeito, os exemplos das posições da ENISA e do OFCOM. A este propósito, esclarece-se que:
   a) O Capítulo III-A da Diretiva Quadro, ao estabelecer o regime comunitário em matéria de segurança e integridade de redes e serviços e não obstante a preocupação expressa no Considerando 44 da Diretiva 2009/140/CE quanto à proteção de infraestruturas críticas (PIC) numa aparente indicação do caminho que se deverá seguir, não introduz qualquer distinção quanto às redes e aos serviços abrangidos;
   b) No mesmo sentido, as disposições constantes do Capítulo V do Título III da LCE, que transpuseram o referido Capítulo III-A da Diretiva Quadro, e, em particular e no que reporta ao objeto desta decisão, o artigo 54.º-B e a alínea b) do artigo 54.º-E, referem-se às redes de comunicações públicas e aos serviços de comunicações eletrónicas acessíveis ao público, sem procederem a qualquer distinção entre diferentes redes ou serviços;
   c) Consequentemente entende o ICP-ANACOM que, ao abrigo do quadro nacional e comunitário, as obrigações de notificação de violações de segurança ou perdas de integridade e da sua divulgação ao público, nos termos que agora são definidos, devem ser aplicáveis a todas as redes de comunicações públicas e a todos os serviços de comunicações eletrónicas acessíveis ao público;
   d) No mesmo sentido, acrescente-se, refere a ENISA que *"in general, considerations about the criticality of an infrastructure served by a telecommunications provider will not be part of the scope of the reporting to ENISA (the rationale being that Critical Infrastructure and Critical Information Infrastructure are not subject to the Regulatory Framework for electronic communications)"*;
   e) O OFCOM preferiu fazer uma aproximação diferente, nas suas linhas de orientação, com base em proposta do CPNI como referido na alínea c) do ponto 5, ou seja, com base em aparente critério relativo a PIC;

f) Neste sentido e conforme fica disposto nas alíneas a) e b) do n.º 4 do Ponto I do Anexo A e nas alíneas a) e b) do n.º 3 do Ponto I do Anexo B, entende o ICP-ANACOM que (i) o impacte de uma violação de segurança ou perda de integridade deve ser aferido por referência a todas as redes e a todos os serviços de uma empresa que sejam afetados pela mesma e (ii) o número de assinantes ou de acessos afetados por uma violação de segurança ou perda de integridade corresponde à soma do número de assinantes ou de acessos que são afetados pela mesma nas várias redes e serviços

Num exemplo e considerando uma violação de segurança ou perda de integridade que atinja uma empresa que ofereça (de uma forma agregada ou não) o serviço telefónico fixo, o serviço de acesso à Internet e o serviço de distribuição de sinal de televisão, atingindo:

i. 10.000 assinantes de serviço telefónico fixo;
ii. 20.000 assinantes de acesso à Internet, e;
iii. 20.000 assinantes de serviço telefónico fixo, de acesso à Internet e de distribuição de sinal de TV;

tendo assim um impacte em 50.000 assinantes de serviços de comunicações eletrónicas (embora por serviço tenha um impacte em 30.000 assinantes de serviço telefónico fixo, 40.000 assinantes do serviço acesso à Internet e 20.000 assinantes do serviço de distribuição de sinal de televisão), o impacte a considerar para os efeitos previstos em ambos os Anexos A e B é de 50.000 assinantes.

10) Refere também a maioria das empresas e a APRITEL ser desadequada a obrigação, prevista no SPD, das empresas informarem o público relativamente a determinados incidentes de segurança invocando, entre outras, razões de ordem legal que alegadamente exigem que a análise do interesse público seja casuística, questões de eventual alarmismo na população que possa resultar dessa divulgação, ou ainda eventual aproveitamento *"sensacionalista"* por parte de alguns *media*, para além de não existir semelhante aproximação por parte de outras ARN's.

Dispondo a alínea b) do artigo 54.º-E da LCE que a ARN pode informar o público pelos meios mais adequados das violações de segurança ou das perdas de integridade ou determinar às empresas que o façam, quando tal seja considerado pela ARN como de interesse público:

a) O ICP-ANACOM entende que a determinação de que a divulgação ao público de uma violação de segurança ou perda de integridade reveste interesse público, pode ser realizada tanto *a posteriori*, após a sua verificação e tendo em conta a sua dimensão e efeitos, como *a priori*, através da prévia fixação das características que, para o efeito, uma violação de segurança ou perda de integridade deve revestir;

b) Neste sentido e por um lado, o ICP-ANACOM procede, nos termos previstos nos n.os 2 e 3 do Ponto I do Anexo B, à fixação das circunstâncias em que considera que o impacte significativo de uma determinada violação de segurança ou perda de integridade, quer pela sua duração, quer pelo número de assinantes ou de acessos afetados (ou pela área geográfica afetada),torna de interesse público a sua divulgação ao público;

c) Por outro lado e nos termos que ficam dispostos no n.º 4 do Ponto I do Anexo B, clarifica ainda o ICP-ANACOM que o disposto neste Anexo não prejudica que, em circunstâncias aí não previstas e sempre que o também considere de interesse público, esta Autoridade possa, *a posteriori*, determinar às empresas que informem o público de violações de segurança ou perdas de integridade ocorridas nas suas redes e serviços;

d) A propósito refira-se que alguns dos incidentes de segurança que nos últimos anos foram notícia nalguns *media*, tanto quanto julgamos saber, até tiveram um impacte inferior (em número de assinantes/acessos afetados) ao último patamar da tabela por nós definida no SPD;

e) As empresas estão certamente dotadas do conhecimento, quer técnico quer comunicacional, que lhes permita informar os seus assinantes e o público em geral duma forma clara, transparente e correta, e desse modo contribuir para evitar eventuais alarmismos ou *"sensacionalismos"*, que poderiam sim verificar-se se essa informação chegasse ao público por outras vias (como por exemplo e rapidamente através das redes sociais, já para não referirmos os exemplos apresentados pelas empresas);

f) Conforme se comprova pela leitura do regulamento da FICORA atrás referido, a aproximação do ICP-ANACOM não é caso único no universo das ARN's europeias.

11) As empresas em geral, e também a APRITEL, classificam o prazo de 30 dias para a implementação das medidas previstas no SPD como escasso, solicitando pelo menos um prazo de 6 meses, após a decisão final.

O ICP-ANACOM, tendo presente as respostas recebidas quanto à importância atribuída pelas empresas à segurança e integridade de redes e serviços, aos investimentos por estas já realizados, e aos procedimentos já implementados, por um lado, bem como as decisões de outros reguladores, e a decisão da Comissão para que as ARN informassem a Comissão e a ENISA quanto aos incidentes de segurança verificados entre 1 de janeiro e 31 de dezembro de cada ano, a entrar em *"velocidade de cruzeiro"* com o relatório remetido durante o 1T2013 e, ainda, havendo agora outras decisões de ARN's como a da PTS – entrada em vigor a 1 de abril de 2012, da decisão de 21 de fevereiro de 2012, e a da FICORA[10] – entrada em vigor a 1 de fevereiro de 2012, da decisão de 23 de janeiro de 2012 e, por último, o tempo decorrido desde a consulta pública efetuada, considera que o prazo solicitado é talvez prolongado.

Pese embora o referido, considerando os argumentos apresentados e procurando conciliar os interesses em presença, o ICP-ANACOM procede ao alargamento do prazo de entrada em vigor das medidas previstas para um período correspondente a 6 meses, nos termos previstos no n.º 1 do Ponto III do Anexo A e no n.º 1 do Ponto III do Anexo B.

No que respeita ao Anexo A, porém, prevê-se, nos termos do n.º 2 do respetivo Ponto III, a obrigação de remessa de relatórios intercalares que cubram todo o período decorrido entre 1 de janeiro de 2013 e a entrada em vigor deste Anexo, com base nos dados disponíveis e tendo por referência as circunstâncias previstas no Ponto I e os requisitos exigidos para a notificação final no número 9 do Ponto II, com vista à respetiva transmissão à Comissão Europeia e à ENISA, na sequência do que tem vindo a ser a postura do ICP-ANACOM em matéria de cooperação com estas instituições.

12) O ICP-ANACOM releva a sua determinação na defesa dos interesses dos cidadãos presente no SPD e bem acolhida pelas associações de consumidores.

13) As entidades públicas que, ao nível central (DGC) e regional (GRM), deram o

[10] Quanto à informação ao público (capítulo 3) a FICORA definiu para a entrada em vigor a data de 1 de abril de 2012.

seu contributo relevam no SPD, a primeira, a defesa dos consumidores e, a segunda, a preocupação havida com a realidade geográfica e político-administrativa das regiões autónomas.

No que respeita ao comentário da DGC relativo à falta de referência ao uso de diferentes tecnologias e às respetivas diferenças ao nível da capacidade de atuação e de resolução de problemas por parte das empresas, importa esclarecer que, ao abrigo do disposto no artigo 54.º-B, no n.º 2 do artigo 54.º-C e na alínea b) do artigo 54.º-E da LCE, não integra o objeto desta decisão a matéria relativa à resolução de violações de segurança ou perdas de integridade, mas apenas e somente a sua notificação e divulgação ao público.

C – CONSIDERAÇÕES ESPECÍFICAS

A) ANEXO A ao SPD

- **AT&T, COLT e Verizon Business**, alertam para o facto de tendo embora eventual cobertura nacional, de uma maneira geral e face à sua especificidade, o seu número de clientes não justificará a qualificação de impacte significativo, solicitando que o ICP-ANACOM retire o critério *"área geográfica"* da decisão.
- Os **CTT** questionam a medição da área geográfica no âmbito das redes móveis.

  Referem também que não estarão abrangidos pela obrigação de notificação (devido à sua especificidade), a necessidade de o ICP-ANACOM clarificar o que se entende por *"empresa"* (I.c) ii) do SPD), e ainda clarificar, respetivamente nas alíneas iii) e iv) do mesmo ponto, *"data que, pela sua relevância"*, e *"impacte geográfico, nomeadamente"* e *"outras entidades relevantes"*.

  Consideram ainda: elevado o número e o prazo da notificação, difícil identificar a causa raiz no prazo estipulado, e uma vez mais que não deveriam estar sujeitos à obrigação de notificar pois *"não disponibilizam ao ICP-ANACOM qualquer informação relativa à rede"*.

  Por último referem que o prazo de implementação deverá ser alargado para 6 meses.
- A **Cabovisão** refere a necessidade de concretizar o conceito de incidente de segurança por referência à continuidade de serviço.

  Considera que os incidentes a reportar deverão ser aqueles com duração a partir de 4 horas, lembrando as propostas do documento da ENISA quanto à expressão entre o número de assinantes afetado e o número total de utilizadores do serviço afetado, e quanto aos serviços elegíveis para notificação.

  Refere dificuldades em determinar área geográfica, em contabilizar impacte de incidentes repetidos, e na cooperação entre empresas.

  Questiona a Cabovisão quanto à notificação de não entrega de chamadas ao 112, no caso de falha de uma interligação quando existem mais, e no caso da causa raiz ser responsabilidade da Portugal Telecom.

Expressa-se quanto à necessidade do ICP-ANACOM definir datas e entidades a que se referem os pontos I.c) iii) e I.d).

Alega excesso de notificações e a necessidade de o regulador fundamentar a necessidade de receber as notificações e a utilização que fará dos relatórios, não aceitando a proposta do regulador quanto a ações corretivas no sentido de evitar reincidências.

Considera que o prazo de notificação deverá ser de 2 dias, e insuficiente um único endereço de correio eletrónico.

"Por razões de segurança jurídica", consideram que deve estabelecer-se uma lista exaustiva de causas raiz de incidentes de segurança.

Por último não lhe é clara a solicitação de que os dados contidos na notificação sejam consonantes com os dados estatísticos remetidos trimestralmente ao ICP-ANACOM, e requerem prazo de implementação alargado para 6 meses.

- O **Grupo ONI** alerta: para a diferença de critérios usados no documento da ENISA, para a consequente confusão entre avarias e incidente de segurança, e para o previsível número de notificações relativas à indisponibilidade do serviço 112, pois qualquer incidente que afete o serviço de voz durante mais de 15 minutos deverá ser notificado.

  Refere-se ainda aos critérios de acumulação de eventos afetando um ou vários operadores, colocando problemas operacionais, aos incidentes em datas especiais, solicitando a sua não inclusão, aos incidentes que afetam redes e serviços nas ilhas das regiões autónomas, lembrando critérios da ENISA de 10% de utilizadores e 4 horas de duração, e à necessidade de se listar as entidades governamentais, regionais e outras socialmente relevantes, para que as empresas não incorram em situações de incumprimento.

  Considera o prazo da notificação inicial curto porque, alega, serve para fins estatísticos, pedindo a sua revisão e alteração para 48 horas, e em demasia 3 notificações, entendendo que a notificação intercalar não deverá existir e a final deverá ser remetida um mês após o final do incidente.

  Por último solicita que o prazo de implementação seja alargado para 6 meses.
- A **Optimus** releva a necessidade de se clarificar quer o tipo de incidentes a reportar, defendendo que devem ser os que afetem a continuidade/disponibilidade do serviço, quer os serviços que cabem no âmbito da notificação, defendendo nomeadamente a exclusão dos serviços de televisão (*"este serviço não foi considerado relevante pela ENISA"*).

Quanto aos patamares requer clarificação de que os mesmos são cumulativos, considera injustificada a notificação de incidentes inferiores a 4 horas, e refere dificuldades na determinação da área afetada.

Quanto às chamadas 112, considera que só os incidentes que impeçam a entrega de chamadas aos PSAP originadas nas redes fixas e com duração igual ou superior a 1 hora devem ser notificados.

Relativamente a incidentes repetidos e a incidentes com impacte nas redes ou serviços de várias empresas, solicita a sua eliminação alegando dificuldades na sua determinação e ainda questões de confidencialidade na segunda hipótese.

Alega iguais dificuldades para incidentes em datas especiais, e solicita reavaliação quanto à notificação de incidentes nas regiões autónomas;

Questiona o exemplo apresentado do SIRESP porque *"este consiste num sistema que deve ser independente dos operadores comerciais de comunicações"*;

Quanto a clientes governamentais ou regionais, para além de alegadas dificuldades na sua implementação, refere constrangimentos legais quanto ao tratamento diferenciado dos vários utilizadores.

Apresenta a seguinte proposta quanto aos incidentes a notificar:

Prazo da Notificação Inicial ▶	Notificação ao ICP-ANACOM		Divulgação ao Público	
	4 horas úteis		4 horas úteis*	
Serviços ▼	duração ≥	PASP ≥	duração ≥	PASP ≥
112 (Fixo)	1	1	4	1
Serviços ▼	duração ≥	clientes ≥	duração ≥	clientes ≥
Voz Fixo	1	450.000		
	2	300.000		
	4	150.000		
	6	60.000		
	8	30.000	8	150.000
Voz Móvel; SMS	1	2.250.000		
	2	1.500.000		
	4	750.000		
	6	300.000		
	8	150.000	8	750.000
Internet (Móvel; Fixo)	1	2.700.000		
	2	1.800.000		
	4	900.000		
	6	360.000		
	8	180.000	8	900.000

Legenda:
Duração - duração expectável mínima do incidente em horas (de acordo com a escala da ENISA)
Clientes - número mínimo de assinantes/acessos afectados
PASP - Ponto de Atendimento de Segurança Pública (Centro de Atendimento do 112)
* Divulgação ao público efectuada só após aprovação/decisão da ANACOM
- Incidentes que se enquadrem neste patamar NÃO devem ser notificados
- Incidentes que se enquadrem neste patamar devem ser notificados

Interpretação da tabela:
1º- Identificar o tipo de serviço
2º- Percorrer, linha a linha, os patamares aplicáveis ao tipo de serviço
3º- Se pelo menos uma linha for verdadeira em ambos os critérios (duração + clientes ou PASP), fixar essa linha
4º- Se a linha estiver assinalada a vermelho, então o incidente deve ser objecto de notificação

Sugere notificação com meios adicionais ao *e-mail* e a utilização de *"mecanismos de autenticação, integridade e não repúdio, como por exemplo a certificação digital"*.

Insiste na alegada dificuldade operacional de, na cooperação entre empresas, aspetos relativos à deteção, avaliação e notificação, e alega eventuais questões de partilha de informação confidencial, propondo a reavaliação desta obrigação.

Quanto à identificação da causa refere dificuldades em caso de fornecedores externos (como a energia).

Solicita esclarecimentos quanto à referência no SPD aos dados estatísticos remetidos trimestralmente ao ICP-ANACOM.

Quanto à notificação inicial discorda do prazo de 2 horas propondo 4 horas; sugere que a *"notificação final"* passe a *"Relatório de Incidente"* e com prazo mais alargado; e põe várias reticências à notificação intercalar, nomeadamente que deveria ser opcional.

- O **Grupo PT** solicita uma definição de *"incidente"*, propondo *"um evento que tem impacto num ou mais elementos de rede com a mesma causa raiz (root cause)"*.

  Refere que deveria ser estabelecido *"que apenas serão objeto de notificação os incidentes que tenham um impacto significativo no funcionamento das redes ou na prestação de serviços ou que afetem a continuidade/disponibilidade das redes e dos serviços"*, e alega eventuais dificuldades na implementação do critério geográfico.

  Defende que os limiares devem ser aplicados por serviço, de acordo com a criticidade dos mesmos, referindo os identificados pela ENISA (Voz Fixa, Voz móvel, SMS, Internet, *E-mail*), reproduzindo a tabela dos patamares constante do documento publicado por aquela Agência:

Duração/ Assinantes/Acessos	1h - 2h	2h - 4h	4h - 6h	6h - 8h	> 8h
1% a 2% de assinantes/acessos					X
2% a 5% de assinantes/acessos				X	X
5% a 10% de assinantes/acessos			X	X	X
10% a 15% de assinantes/acessos		X	X	X	X
> 15% de assinantes/acessos	X	X	X	X	X

  Menciona a possibilidade de existirem situações fronteira relativamente a violação de dados pessoais e que deveriam ser *"excluídos da obrigação de notificação os serviços de suporte que sejam prestados sobre a rede de determinado operador"*.

  Quanto aos incidentes 112 defende, entre outras, que a notificação só seja feita com base na participação de avaria por parte do MAI[11] e, relativamente às chamadas originadas nos móveis, que devem estes ser excluídos pois a chamada poderá ser feita através de outro operador.

  Relativamente ao ponto I.c), referem, respetivamente: (i) nada contra se o regulador seguir as suas propostas/tabela, caso contrário é desajustado; (ii) afigura-se inviável e propõem a sua retirada; (III) datas relevantes devem ser previamente definidas e divulgadas pelo ICP-ANACOM, e para incidentes superiores a uma hora; (iv) deve ser para eventos com duração superior a uma hora.

[11] Ministério da Administração Interna.

Refere o Grupo PT relativamente ao ponto I.d) que, nos contratos celebrados com as entidades mencionadas, tem cláusulas de confidencialidade pelo que deverá ser o ICP-ANACOM a recolher junto dessas entidades a informação requerida.

O Grupo PT considera o processo de notificação excessivamente burocrático, sendo, em sua opinião, essencial definir a quem cabe coordenar a cooperação entre empresas, e que a notificação seja feita após a resolução do incidente;

Entende que a submissão por correio eletrónico não garante os meios de segurança necessários, pelo que deve ser implementado processo que o faça;

Não lhe é percetível o sentido e o alcance da menção a *"dados estatísticos disponibilizados trimestralmente ao ICP-ANACOM"*, dadas as finalidades específicas e determinadas dos dados fornecidos pelas empresas.

Sugere que seja criado um *"template"* para notificações para harmonização dos relatórios das empresas com essa obrigação, incluindo os MVNO's, e reafirma a necessidade de articulação de procedimentos nesta matéria tendo presente a Diretiva Privacidade.

Por último propõe que o prazo de notificação inicial deve ser alargado para 8 horas úteis, o prazo da notificação intercalar deve passar para 8 horas úteis após o fim do incidente (se o fim deste não constar da notificação inicial), e que a informação a disponibilizar na notificação final deve revestir caráter facultativo; apela ao ICP-ANACOM que considere prazo de implementação de, no mínimo, 6 meses.

- A **Vodafone "I.I.C. [Início de Informação Confidencial]**
  F.I.C. [Fim de Informação Confidencial]
- A **APRITEL** considera introdutoriamente que apenas devem ser notificados incidentes que provoquem interrupção do serviço, e não incidentes que afetem temporariamente a qualidade de serviço, que os critérios devem ser em linha com *"as orientações dadas pela ENISA"*, e que os procedimentos são demasiado exigentes, pondo a hipótese de um elevado volume de notificações que *"pode inclusive implicar um congestionamento do sistema do Regulador"*.

  Refere que no SPD não consta quais os serviços elegíveis para notificação, e *"entende que o ICP-ANACOM deve esclarecer qual o entendimento relativo a operações de manutenção preventivas e/ou corretivas ou melhorias de rede programadas"*.

Considera patamares definidos excessivamente curtos, referindo como exemplo que *"alguns incidentes tão curtos, de 15 minutos, poderão não ser detetáveis"*.

Entende que para a avaliação do impacto se deve considerar apenas *"assinantes/acessos"* pois a sua conjugação com *"área geográfica"* torna o processo demasiado exaustivo e complexo, e refere impossibilidade de determinar clientes afetados no serviço móvel.

Quanto ao impacte no acesso ao número único de emergência considera que, no caso dos serviços fixos se deve seguir a ENISA quanto à combinação de percentagem de assinantes/acessos afetados e duração do incidente e, no caso dos móveis, se não deve considerar pois se uma rede está indisponível as chamadas podem ir através de uma outra rede móvel.

Considera inexequível a notificação de incidentes repetidos no tempo (I.c) (i)), e com impacte acumulado em várias empresas (I.c) (ii)); considera que quanto a datas especiais devem as empresas ser previamente informadas (I.c) (iii)), e quanto a entidades governamentais e regionais (I.d)), que será necessário definir uma lista prévia, que o exemplo do SIRESP é questionável pois *"a falha dos serviços dos operadores não deve impactar o SIRESP"*, e que importa acautelar questões legais pois *"impende sobre os operadores uma obrigação de não discriminação"*.

Entende que o número de notificações é excessivo, não tendo paralelo nas posições assumidas pela ENISA ou por outros reguladores, como o OFCOM, questionando *"a necessidade ou utilidade de receção de tal número de notificações pelo ICP-ANACOM que, em última análise, poderá não ter capacidade para analisar (ou sequer receber) tanta informação"*.

A APRITEL considera que a notificação por *e-mail* não basta, e que o conteúdo deverá ser salvaguardado; que não é exequível para as empresas a cooperação com vista à notificação de um mesmo incidente de segurança; e que quando a causa é falha num fornecedor de serviços externo (fornecedor de energia ou outro operador), nem sempre é possível obter a curto/médio prazo a informação das causas e do tempo estimado de resolução.

Sugerem que a notificação inicial seja feita num prazo de 2 dias úteis e que a notificação final passe a designar-se por *"Relatório de Incidente"*.

Sugere que seja adotado um *"template"* comum e refere que, se não se delimitarem os serviços elegíveis e se não se flexibilizarem os critérios de duração e do número de assinantes ou área afetada, os seus associados terão

de canalizar esforços para a elaboração de relatórios desviando o foco do fundamental (assegurar manutenção da rede e dos serviços).

Por último classifica como inviável e inaceitável o prazo de 30 dias para entrada em vigor, propondo mínimo de 6 meses.

- O **GRM** face à condição ultra periférica da Madeira considera que *"poderá justificar-se uma redução dos escalões subjacentes aos critérios do número de assinantes/acessos e/ou área geográfica da referida tabela"*.

ENTENDIMENTO DO ICP-ANACOM

Apresenta-se seguidamente os fundamentos que suportam a versão final do Anexo A, destacando-se, antes de mais e no essencial, as seguintes alterações:

- Ajustamentos nos patamares da tabela constante da alínea a) do n.º 3 do Ponto I, quer no que respeita à duração, quer ao número de assinantes ou de acessos afetados (ou área geográfica afetada);
- Eliminação da obrigação de notificação por parte de um conjunto de empresas atingidas pela mesma violação de segurança ou perda de integridade, com exceção da circunstância agora prevista na alínea g) do n.º 3 do Ponto I;
- Fixação do início da contagem do prazo para a notificação inicial no momento da verificação da circunstância que, no caso concreto, determinou a obrigação de notificação, nos termos previstos no n.º 4 do Ponto II, deixando assim de haver dúvidas quanto à existência de impacte significativo no momento dessa notificação;
- Clarificação das circunstâncias que constituem um impacte significativo e determinam a obrigação de notificação, nos termos previstos nos n.os 2 e seguintes do Ponto I, salientando-se a restrição do critério relativo à *"área geográfica afetada"* aos casos em que o critério relativo ao número de *assinantes ou de acessos afetados* seja inaplicável ou, no caso concreto, fundamentadamente impossível de determinar ou estimar, de acordo com o disposto na alínea e) do n.º 4 do Ponto I;
- Alargamento do prazo de entrada em vigor a um período correspondente a seis meses, conforme previsto no n.º 1 do Ponto III;
- Previsão, a título transitório e nos termos previstos no n.º 2 do Ponto III, de uma obrigação de remessa de relatórios relativamente ao período entre 1 de janeiro de 2013 e a entrada em vigor deste Anexo A.

1. O novo quadro regulatório em matéria de segurança e integridade de redes e serviços, tal como resulta do disposto no capítulo III-A da Diretiva Quadro e, entre nós, do Capítulo V do Título III da LCE, e em especial a matéria objeto do SPD, apresenta fundamentalmente características de transparência, quer no que respeita à notificação de violações de segurança ou perdas de integridade às ARN e ao respetivo reporte anual por parte destas à Comissão Europeia e à ENISA, quer no âmbito da divulgação das mesmas ao público por parte da ARN ou, quando assim o seja determinado, pelas próprias empresas (antes muitas vezes apenas divulgadas por notícias, por vezes pouco claras e/ou pouco precisas, nos *media*).
2. Um ponto que queremos deixar bem expresso é que não é expectável, nem desejável, um número muito elevado de notificações, ou um número muito reduzido de notificações que leve a perder-se o objetivo em vista numa matéria que é recente no quadro regulatório, para o que é conveniente um número de notificações que permita retirar conclusões com alguma solidez e significado, sem prejuízo da possibilidade de no futuro serem revistas as dimensões agora usadas para balizar o impacte significativo, e que obriga à notificação, com vista à sua melhoria como aliás já referido no SPD.
3. Atente-se que não há, no nosso entendimento, qualquer confusão entre avarias e incidentes de segurança, pois uma avaria está incluída nos incidentes de segurança (por exemplo, se de *hardware*, a causa raiz estará incluída na categoria *"falha de hardware"*).

   Relativamente ao nosso entendimento relativo a *"operações de manutenção preventivas e/ou corretivas ou melhorias de rede programadas"*[12], só poderá ser um: havendo como consequência um impacte significativo, tem de ser notificado.
4. Quanto à proposta do Grupo PT de uma definição de *"incidente"*, entendemos

[12] Não fará, em princípio, sentido que medidas destas tenham um impacte significativo; por outro lado, já tivemos conhecimento de várias destas ações, em que era pois suposto não haver impacte significativo, mas das quais resultaram incidentes de segurança com impacte significativo nomeadamente, e por exemplo, por alegado erro humano.

pelas razões já referidas não acolher, até porque por exemplo a Recomendação E.409 da UIT[13], define *"evento"*, *"incidente"*, e *"incidente de segurança"*, e não foi considerada na Diretiva, ou seja, terá sido ali considerado não restringir, mediante uma definição, o âmbito dos incidentes de segurança passíveis de notificação.

5. No que respeita à identificação das violações de segurança ou perdas de integridade a notificar e nos termos previstos no n.º 2 do Ponto I do Anexo A, considera-se que devem ser objeto de notificação todas as violações de segurança ou perdas de integridade que causem uma perturbação grave no funcionamento das redes e serviços, com impacte significativo na continuidade desse funcionamento, de acordo com as circunstâncias e as regras previstas nos n.os 3 e seguintes do mesmo Ponto I.
6. Para a avaliação do impacte de uma determinada violação de segurança ou perda de integridade e a consequente aferição do seu caráter significativo ou não significativo, deve, nos termos definidos nas alíneas do n.º 4 do Ponto I do Anexo A, atender-se às seguintes regras:
   a) O impacte de uma violação de segurança ou perda de integridade deve ser aferido por referência a todas as redes e a todos os serviços de uma empresa que sejam afetados pela mesma;
   b) O número total de assinantes ou de acessos afetados por uma violação de segurança ou perda de integridade corresponde à soma do número de assinantes ou de acessos que são afetados pela mesma nas várias redes e serviços[14];
   c) O número de assinantes de um serviço que seja suportado noutro serviço só será contabilizado quando o serviço de suporte não tiver sido afetado[15];
   d) O número de assinantes ou de acessos afetados corresponde ao número de assinantes ou de acessos que sejam abrangidos pela violação de segurança ou perda de integridade (ou, por outras palavras, o número de assinantes ou de acessos a quem são potencialmente disponibilizados as redes ou serviços em situação de

[13] União Internacional de Telecomunicações.
[14] *Vide* exemplo na alínea f) do ponto 9 das nossas posições relativas às *"considerações gerais"*.
[15] Por exemplo para o caso do SMS, só conta no caso do serviço telefónico de suporte não ser afetado.

funcionamento normal), ou, na impossibilidade da sua determinação, a uma estimativa baseada nos elementos estatísticos detidos pela empresa;

e) O critério relativo à área geográfica afetada só deve ser aplicado caso o critério relativo ao número de assinantes ou de acessos afetados seja inaplicável ou, no caso concreto, fundamentadamente impossível de determinar ou estimar, o que, porventura, será o caso dos serviços de teledifusão;

f) As circunstâncias previstas no n.º 3 do Ponto I do Anexo A devem ser aferidas em relação a uma empresa individualmente considerada, ou, no caso das circunstâncias previstas na alínea a) e, na parte que remete para esta alínea, na alínea c), ambas do mesmo n.º 3, também em relação a um conjunto de empresas que se encontrem nas condições previstas no n.º 2 do artigo 3.º da Lei n.º 19/2012, de 8 de maio. Esta opção, tendo em conta o disposto no artigo 54.º-B da LCE, fundamenta-se na necessidade de obtenção de informação relativamente à dimensão global de um determinado incidente que, no seu impacte sobre as empresas integradas num conjunto de empresas nestas condições, atingiu um impacte significativo, assumindo o ICP-ANACOM como proporcional e adequado que, para esse fim, se exija a tais empresas que, de acordo com o disposto no n.º 13 do Ponto II do mesmo Anexo A, se coordenem na sua deteção, avaliação e notificação conjunta.

7. Do que conhecemos, nomeadamente os documentos da ENISA e do OFCOM e os regulamentos da FICORA e da PTS, podemos conceder que este entendimento em parte e aparentemente não encontra paralelo noutro regulador europeu, mas estamos convictos de que esta é a correta interpretação do disposto na lei, sob pena de não serem notificados incidentes de segurança com impacte significativo num elevado número de utilizadores, só porque estes utilizam diferentes serviços ou um mesmo serviço suportado em diferentes redes, tendo no entanto uma causa comum - o mesmo incidente de segurança.
8. Relativamente à alínea a) do Ponto I do Anexo A do SPD, agora alínea a) do n.º 3 do Ponto I do Anexo A, esclarece-se o seguinte:

a) Os critérios *"duração"*, por um lado, e *"número de assinantes ou de*

acesso afetados (ou nos termos da alínea e) do n.º 4 do Ponto I, área geográfica afetada)" são cumulativos, conforme resulta da conjunção *"e"*, já constante do SPD e agora mantida na versão final da decisão;

b) Manteve-se o número de patamares, mas adaptados, relevando-se que a maior diferença reside no subcritério *"area geográfica afetada"*, tendo presente que, nos termos do disposto na alínea e) do n.º 4 do Ponto I do Anexo A e atentos os comentários recebidos a este propósito, a aplicação deste critério[16] é agora supletiva, apenas para os casos em que o critério relativo ao número de assinantes ou de acessos afetados seja inaplicável ou, no caso concreto, fundamentadamente impossível de determinar ou estimar;

c) A proposta do Grupo PT neste ponto segue a proposta da ENISA a qual, tendo um objetivo diverso e relevando um racional diferente do que resulta da interpretação do ICP-ANACOM do disposto na LCE, não se acolhe;

d) Quanto à proposta da Optimus, se a seguíssemos, estaríamos a conceder a hipótese da rede desta empresa poder estar inoperacional durante um período de até quatro (4) horas, sem obrigação de notificação, o que não faz sentido.

9. Relativamente à alínea b) do Ponto I do Anexo A do SPD, agora alínea b) do n.º 3 do Ponto I do Anexo A, entende-se o seguinte:

a) A acrescentar ao referido no ponto anterior, há que considerar, antes de mais, a competência cometida ao ICP-ANACOM relativamente ao número único de emergência europeu 112, ao abrigo do disposto no artigo 5.º[17] do Decreto-Lei n.º 73/97, de 3 de abril, assim como o disposto no n.º 2 do artigo 49.º da LCE quanto ao dever das empresas que prestam serviços telefónicos acessíveis ao público de tomar todas as medidas necessárias para assegurar o acesso ininterrupto aos serviços de emergência;

[16] Que no entanto deve continuar a ser estimado e referido, no mínimo, na notificação final.

[17] *"Ao Ministério do Equipamento, do Planeamento e da Administração do Território, através do Instituto das Comunicações de Portugal, compete coordenar com os operadores de telecomunicações de uso público a adaptação da rede básica de telecomunicações e das redes do serviço móvel terrestre de forma que as chamadas feitas para o n.º 112 sejam atendidas numa central de emergência."*

b) O que está aqui em causa é a conetividade das empresas, direta ou indiretamente (através de outra empresa a que esteja interligada), aos serviços de emergência;

c) Não faz sentido que uma empresa que oferece uma rede móvel fique isenta de notificação como pretende nomeadamente a APRITEL, com o argumento de que as chamadas para o 112 poderão sair por outra rede caso a rede nativa esteja indisponível, desde logo porque: as chamadas de emergência podem ser efetuadas também através do ainda número nacional de emergência 115, ou a rede não ser afetada na sua parte rádio mas sim na parte *core* e neste caso não temos a informação de que esteja garantido o que refere a APRITEL; por outro lado poderia acontecer que também as outras redes móveis não pudessem entregar as chamadas de emergência e então, nesse caso, ninguém notificava; e ainda, como já referido, porque importa ter o conhecimento do que acontece nas redes e serviços de comunicações eletrónicas em termos de segurança e integridade;

d) Tenha-se ainda em atenção o que sobre esta matéria diz o documento da ENISA *"This can be a stand-alone parameter meaning that if an incident impacts on emergency calls, the reporting scheme is triggered regardless of the duration or users affected"*, e que neste caso seguimos, concedendo embora que, e apenas para efeitos de notificação e neste momento, se considerem apenas os incidentes de segurança com duração igual ou superior a 15 minutos;

e) No caso de falha de uma interligação quando existem mais como questionado pela Cabovisão, desde que a empresa continue a entregar noutro ponto as chamadas dirigidas aos PASP[18], não será obrigada a notificar; quanto à possibilidade de o incidente de segurança poder ter a *"root cause"* na Portugal Telecom como coloca também a Cabovisão, entende-se que, neste momento, quem deixa de assegurar aos seus assinantes o acesso ininterrupto aos serviços de emergência deve sempre notificar, sem prejuízo da outra empresa também o poder fazer e não esquecendo que as responsabilidades das empresas em matéria de segurança e integridade das redes e serviços não se esgotam na notificação;

[18] Pontos de Atendimento de Segurança Pública (Centros de Atendimento do 112/115).

f) Concluindo, se uma empresa não consegue entregar diretamente aos PASP ou indiretamente através de outra empresa com quem tem interligação, as chamadas para o 112[19], tem de notificar.

10. Relativamente à alínea c) do Ponto I do Anexo A do SPD, agora alíneas c), d), e) e g) do n.º 3 do Ponto I do Anexo A, é nosso entendimento que:

a) No que respeita ao item i) da alínea c) do Ponto I do Anexo A do SPD, agora alínea c) do n.º 3 do Ponto I do Anexo A, importa conhecer, analisar e eventualmente tomar medidas relativamente a um determinado incidente de segurança que, repetindo-se num espaço de tempo de quatro[20] semanas, tenha um impacte significativo acumulado enquadrável numa das circunstâncias previstas nas alíneas a) ou b) do mesmo n.º 3 do Ponto I, para tal devendo ser considerados os incidentes de segurança que tenham a mesma origem, nomeadamente quanto à causa raiz e quanto ao(s) elemento(s) de rede ou sistema afetado(s);

b) No que respeita ao item ii) da alínea c) do Ponto I do Anexo A do SPD, não se inclui nesta decisão final a obrigação de notificação do incidente de segurança que impacte significativamente em várias empresas, com exceção da situação agora prevista na alínea g) do n.º 3 do Ponto I do Anexo A;

c) No que respeita ao item iii) da alínea c) do Ponto I do Anexo A do SPD, agora alínea d) do n.º 3 do Ponto I do Anexo A, importa ainda conhecer, analisar e eventualmente tomar medidas relativamente a um determinado incidente de segurança que tenha uma duração igual ou superior a uma hora e afete um número de assinantes ou de acessos igual ou superior a 1.000 ou, nos termos da alínea e) do número 4 do mesmo Ponto I, uma área geográfica igual ou superior a 100 km2, quando esse incidente de segurança se verifique em datas nas quais seja particularmente relevante o normal e contínuo funcionamento das redes e serviços, em particular as datas já identificadas nos termos do n.º 5 do mesmo Ponto I e as que, de acordo com o disposto neste mesmo número, venham a ser identificadas pelo ICP-ANACOM;

d) No que respeita ao item iv) da alínea c) do Ponto I do Anexo A do SPD,

[19] Inclui as chamadas efetuadas mediante a marcação do 115.
[20] Considerou-se que é preferível estabelecer um prazo determinado de 4 semanas, sempre igual, do que de um (1) mês, variável.

agora alínea e) do n.º 3 do Ponto I do Anexo A, devido à especificidade das regiões Autónomas dos Açores e Madeira (compostas por ilhas) e atentos os comentários do GRM, entende o ICP-ANACOM que importa ser notificado dos incidentes de segurança que ali aconteçam com duração igual ou superior a 30 minutos e que impactem no funcionamento de todas as redes e serviços oferecidos por uma mesma empresa na totalidade do território de uma ilha (ou seja, quando uma empresa fique impedida de continuar a disponibilizar aos utilizadores toda a sua oferta numa determinada ilha), independentemente do número de assinantes ou de acessos afetados e da área geográfica afetada.

11. Não podemos deixar de relevar o disposto no Considerando 44 da Diretiva 2009/140/CE: *"A comunicação fiável e segura de informações através de redes de comunicações eletrónicas é cada vez mais fundamental para toda a economia e para a sociedade em geral. A complexidade dos sistemas, as falhas técnicas ou erros humanos, os acidentes ou os ataques aos sistemas podem, todos eles, ter consequências no funcionamento e na disponibilidade das infraestruturas físicas através das quais se fornecem serviços importantes para os cidadãos da UE, incluindo serviços de governo eletrónico"*.

    Este é o racional subjacente à alínea d) do Ponto I do Anexo A do SPD, e que está quanto a nós no espírito dos quadros comunitário e nacional, quando ali se dispõe, respetivamente no n.º 1 do artigo 13.º-A da Diretiva Quadro e no n.º 1 do artigo 54.º-A da LCE, que devem ser tomadas medidas para impedir ou minimizar o impacte dos incidentes de segurança nos utilizadores e nas *"redes interconectadas"* ou *"redes interligadas"*, Em particular, os termos *"redes interconectadas"* ou *"redes interligadas"* não se restringem, neste caso e no entendimento do ICP-ANACOM, apenas à *interconecção*/*interligação* de redes de comunicações públicas, antes integrando as redes / *"infraestruturas físicas através das quais se fornecem serviços importantes para os cidadãos da UE, incluindo serviços de governo eletrónico"*, serviços estes que se suportam em redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público e que, para servirem os cidadãos, necessitam de comunicações fiáveis e seguras.

    Assim e atentas as atribuições e as competências cometidas a esta Autoridade em matéria de segurança e de emergência, entende o ICP-

ANACOM que deve ser notificado de qualquer violação de segurança ou perda de integridade, detetada pelas empresas ou a estas comunicada pelas entidades clientes, que impacte no funcionamento das redes e serviços através dos quais sejam prestados serviços relevantes à sociedade e aos cidadãos, por parte de entidades públicas ou privadas, de âmbito nacional ou regional, previstas no n.º 6 do mesmo Ponto I, desde que tenha uma duração igual ou superior a 30 minutos.

Ainda neste ponto e no que respeita às obrigações de confidencialidade a que o Grupo PT afirma encontrar-se sujeito e que o *"impedem de partilhar informação, qualquer que ela seja"*, esclarece-se que:

a) Nos termos do disposto no n.º 1 do artigo 108.º da LCE, as entidades que estão sujeitas a obrigações nos termos deste diploma devem prestar ao ICP-ANACOM todas as informações relacionadas com a sua atividade, para que esta Autoridade possa exercer todas as competências previstas na lei;
b) A informação a transmitir enquadra-se na obrigação de notificação ao ICP-ANACOM decorrente do disposto no artigo 54.º-B da LCE, sendo necessária ao exercício das competências que nesta matéria são cometidas a esta Autoridade, não podendo, como tal, ser à partida excluída com fundamento numa obrigação de confidencialidade de origem exclusivamente contratual;
c) As empresas sujeitas à obrigação de notificação devem identificar, de forma fundamentada, as informações que consideram confidenciais e juntar, caso se justifique, uma cópia não confidencial dos documentos em que se contenham tais informações, nos termos do disposto no n.º 3 do artigo 108.º da LCE e em conformidade com a deliberação desta Autoridade de 17 de novembro de 2004; e
d) O ICP-ANACOM encontra-se sujeito a exigências de confidencialidade, nos termos do Código de Procedimento Administrativo, da Lei n.º 46/2007, de 24 de agosto, da LCE, dos seus Estatutos, aprovados pelo Decreto-Lei n.º 309/2001, de 7 de dezembro, e da demais legislação aplicável.

Contudo, porque se concede que importa analisar as várias envolventes com os vários interessados nesta questão e nos termos que ficam previstos no n.º 6 do Ponto I do Anexo A, a identificação das entidades relevantes para os

efeitos previstos na alínea f) do n.º 3 do mesmo Ponto I será posteriormente assegurada pelo ICP-ANACOM e devidamente notificadas às empresas com uma antecedência mínima de cinco dias úteis. A única exceção que neste momento se considera que importa ficar desde já definida é a relativa ao Sistema Integrado das Redes de Emergência e Segurança de Portugal (SIRESP) o qual, ao contrário do que é referido pela Optimus e APRITEL, não é independente dos serviços das empresas, conforme o ICP-ANACOM teve oportunidade de comprovar durante o exercício PROCIV V, organizado pela ANPC[21] em 17 de novembro de 2011.

Por último e no que respeita à posição da OPTIMUS no sentido de que cumpre *"acautelar questões legais quanto ao tratamento diferenciado dos vários utilizadores, dado que (…) recai sobre os operadores a obrigação de não discriminação dos clientes finais"*, esclarece-se que a circunstância prevista na alínea f) do n.º 3 do Ponto I do Anexo A se justifica pela relevância dos serviços prestados à sociedade e aos cidadãos pelos utilizadores finais em causa, relevância esta que, em obediência ao princípio da igualdade na sua vertente material, exige, nesta matéria, um tratamento diferenciado em relação aos demais utilizadores finais.

12. Quanto ao número de notificações, temos o seguinte entendimento:
    a) Haverá lugar a uma notificação inicial, a uma notificação de fim de violação de segurança ou perda de integridade com impacte significativo, dada a relevância do conhecimento do fim do impacte significativo, e a uma notificação final;
    b) Nas circunstâncias previstas nas alíneas c) e g) do n.º 3 do Ponto I do Anexo A, as empresas submetem, respetivamente, apenas uma notificação final ou podem submeter uma única série de notificações, conforme agora disposto nos n.ºs 2 e 3 do Ponto II do Anexo A, e face ao carácter específico das situações a que se referem.
    c) Não se acolhe, por agora, a proposta de um *template* semelhante ao proposto no documento da ENISA (que não é para o mesmo efeito) ou no documento do OFCOM, pois considera-se neste momento prematuro fazê-lo, e também não foi essa a opção da FICORA ou da PTS;
13. Nos termos previstos no n.º 12 do Ponto II do Anexo A, as notificações inicial

[21] Autoridade Nacional de Proteção Civil.

e de fim de violação de segurança ou perda de integridade com impacte significativo devem ser efetuadas quer através de correio eletrónico, quer através de contacto telefónico imediatamente a seguir, ambos dentro do prazo estabelecido; o contacto telefónico servirá para notificar com a informação relevante, caso haja problemas com o correio eletrónico, ou para confirmar a receção da informação por aquele meio. A notificação final deve ser efetuada através de entrega em mão ou de correio registado;

14. Num tempo em que a partilha de informação, nomeadamente em matéria de segurança, é considerada essencial para a devida resposta aos desafios que se colocam neste âmbito às empresas e entidades interessadas nesta matéria (como por exemplo nas redes CSIRT[22], como sublinhado pela APRITEL), mantemos o disposto no SPD quanto a um dever de cooperação entre as empresas cujas redes ou serviços sejam impactados no seu funcionamento pela mesma violação de segurança ou perda de integridade, para uma correta deteção e avaliação de impacte dessa violação de segurança ou perda de integridade e, no caso previsto na alínea g) do número 3 do Ponto I do Anexo A, para a respetiva notificação, conforme previsto no n.º 13 do Ponto II do mesmo Anexo A.
15. No que respeita ao disposto na alínea d) do n.º 5, na alínea a) do n.º 7, na alínea e) do n.º 9 e no n.º 10 do Ponto II, recomenda-se que as causas raiz sejam reportadas ao ICP-ANACOM em conformidade com as listas constantes do documento *"Technical Guidelines on Incident Reporting"*, publicado pela ENISA sempre que aplicável.
16. A obrigação de sujeição da informação a notificar ao ICP-ANACOM, sempre que possível, às definições fixadas no âmbito das obrigações de entrega de informação periódica ao ICP-ANACOM, prevista no n.º 11 do Ponto II, justifica-se pela necessidade de tentar seguir o que naquela sede já está harmonizado de modo a ser possível ao ICP-ANACOM fazer a devida análise, em termos de número de assinantes ou de acessos.
17. A prioridade concedida pela parte final do n.º 4 do Ponto II à mitigação e à resolução da violação e segurança ou perda de integridade em relação à sua notificação inicial tem como limite a obrigação de notificação em tempo ao ICP-ANACOM, conforme na mesma sede fica expressamente ressalvado.
18. Em conformidade com o disposto no artigo 54.º-B da LCE, entende o ICP-

[22] *Computer Security Information Response Team*.

ANACOM dever clarificar que a obrigação de notificação de violações de segurança ou perdas de integridade com impacte significativo pressupõe, necessariamente, uma obrigação de proceder à avaliação prévia do impacte dos incidentes ocorridos, obrigação esta de cujo cumprimento as empresas não se podem, em qualquer caso, eximir, nem tão pouco transferir para o ICP-ANACOM.

Neste sentido, nos termos do disposto no novo n.º 14 do Ponto II do Anexo A e tendo em vista o cabal cumprimento do disposto neste Anexo A, determina-se que cabe às empresas implementar todos os meios e os procedimentos necessários à deteção, à avaliação do impacte e à notificação das violações de segurança ou perdas de integridade que preencham as circunstâncias previstas no Ponto I do mesmo Anexo A.

19. Relativamente aos prazos de notificação, releva-se o seguinte:
    a) Os prazos de notificação ao ICP-ANACOM devem facilitar a análise de impacte significativo pelas empresas através da duração real e não da expectável como acontecia no SPD;
    b) Assim e nos termos previstos no n.º 4 do Ponto II, a notificação inicial deve ser enviada logo que seja possível e desde que a empresa possa concluir que existe ou existirá impacte significativo, até uma hora após a verificação da circunstância prevista no Ponto I que, no caso concreto, determinou a obrigação de notificação, ou seja e por outras palavras, até uma hora após o termo da duração que, no caso concreto, determinou a obrigação de notificação, deixando assim de fazer sentido a hipótese, colocada no SPD, de o incidente de segurança poder não atingir um impacte significativo;

    c) Para os efeitos previstos no n.º 3 do Ponto I, a duração de uma determinada violação de segurança ou perda de integridade e os prazos de notificação são contínuos, não sendo acolhida a proposta no sentido da sua contagem em horas úteis;
    d) A notificação intercalar desaparece enquanto tal, passando a ter a forma de notificação de fim de incidente de segurança com impacte significativo, a apresentar ao ICP-ANACOM logo que possível, dentro do prazo máximo de duas horas após a perda de impacte significativo, salvo quando esta tenha já sido comunicada na notificação inicial, conforme previsto no n.º 6 do Ponto II;

e) Nos termos previstos no n.º 8 do Ponto II, a notificação final deve ser enviada ao ICP-ANACOM no prazo de vinte dias úteis a contar do momento em que a violação de segurança ou perda de integridade deixa de assumir um impacte significativo, o que pode não coincidir com a total resolução do incidente de segurança. Concede-se assim um prazo substancialmente maior para esta notificação final, de modo a que a informação venha o mais completa e detalhada possível, tentando evitar novas iterações entre o ICP-ANACOM e as empresas.

20. Quanto ao conteúdo das notificações, salienta-se o nosso entendimento relativamente aos seguintes pontos:
    a) Apesar de, neste momento, se considerar para efeito de impacte significativo o critério *"área geográfica afetada"* apenas como supletivo, nos termos previstos na alínea e) do n.º 4 do Ponto I, importa ainda assim estimar a área geográfica impactada, razão pela qual se exige a sua indicação no âmbito da notificação final, de acordo com o disposto no item v) da alínea d) do n.º 9 do Ponto II, e, sendo possível estimar, da notificação inicial, nos termos do item iv) da alínea e) do n.º 5 do mesmo Ponto;
    b) A notificação inicial deve conter a informação prevista nas alíneas a) a d) do n.º 5 do Ponto II, bem como a estimativa possível do seu impacte em termos de redes e serviços afetados, acesso aos serviços de emergência, número de assinantes ou de acesso afetados e área geográfica afetada, conforme exigido na alínea e) do mesmo número;
    c) A todo o tempo, ao abrigo e nos termos do disposto nos artigos 108.º e 109.º e tendo presente o n.º 2 do artigo 54.º-G e o artigo 112.º da LCE, o ICP-ANACOM poderá solicitar informação relativa ao incidente de segurança, nomeadamente através dos contactos fornecidos pela empresa na notificação inicial;
    d) A notificação final deve conter, com detalhe, a informação prevista no n.º 9 do Ponto II do Anexo A, nomeadamente, entre outros pontos, quanto:
        1) Às causas raiz, nos termos previstos na alínea e) do mesmo número 9, recomendando-se a utilização, sempre que aplicável, da lista constante do documento "*Technical Guidelines on Incident Reporting*", publicado pela ENISA;

2) A todas as redes e a todos os serviços afetados e, dentro de cada rede ou serviço, o número de assinantes ou de acessos afetados e a percentagem que esse número representa em relação ao total de assinantes ou de acessos, nos termos previstos nos itens iii) e iv) da alínea d) do mesmo n.º 9;

3) Às medidas referidas nas alíneas f) a h) do mesmo n.º 9 as quais, ao contrário do que é referido pela Cabovisão, são determinantes para a garantia da segurança e integridade de redes e serviços.

21. Quanto à entrada em vigor, para lá do já referido e atentos os ajustes introduzidos no texto da decisão final face ao texto do SPD, releva-se que, face às obrigações que se mantêm quer para as empresas quer para o ICP-ANACOM, as empresas devem notificar o ICP-ANACOM das violações de segurança ou perdas de integridade verificadas até àquela data nos moldes previstos na disposição transitória no n.º 2 do ponto III do Anexo A.
22. Por razões de maior clareza e precisão reformulou-se o Anexo A, privilegiando em particular um rearranjo das disposições ali contidas.

VERSÂO FINAL DO ANEXO A:

Circunstâncias, formato e procedimentos aplicáveis às exigências de comunicação de violações de segurança ou perdas de integridade com impacte significativo no funcionamento das redes de comunicações públicas e dos serviços de comunicações eletrónicas acessíveis ao público

I. Circunstâncias

1. Nos termos do disposto no artigo 54.º-B da Lei n.º 5/2004, de 10 de fevereiro, alterada e republicada pela Lei n.º 51/2011, de 13 de setembro (doravante a "Lei das Comunicações Eletrónicas"), todas as empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público (doravante, as «empresas») estão obrigadas a notificar o ICP – Autoridade Nacional de Comunicações (ICP-ANACOM) das violações de segurança ou das perdas de integridade com impacte significativo no funcionamento das redes e serviços que oferecem.

2. Devem ser objeto de notificação todas as violações de segurança ou perdas de integridade que causem uma perturbação grave no funcionamento das redes e serviços, com impacte significativo na continuidade desse funcionamento, de acordo com as circunstâncias e as regras previstas nos números seguintes.

3. Para efeitos do disposto nos números anteriores, as empresas devem notificar o ICP-ANACOM:

a) De qualquer violação de segurança ou perda de integridade cujo impacte se inclua num dos seguintes patamares:

Duração, e	**Número de assinantes ou de acessos afetados** **(ou, nos termos da alínea e) do n.º 4 do Ponto I, área geográfica afetada)**
≥ 30 minutos	n.º de assinantes ou de acessos afetados ≥ 500.000 (ou, nos termos da alínea e) do n.º 4 do Ponto I, área geográfica afetada ≥3.000 km2)

≥ 1 hora	500.000 > n.º de assinantes ou de acessos afetados ≥ 100.000 (ou, nos termos da alínea e) do n.º 4 do Ponto I, 3.000 km2 > área geográfica afetada ≥ 2.000 km2)
≥ 2 horas	100.000 > n.º de assinantes ou de acessos afetados ≥ 30.000 (ou, nos termos da alínea e) do n.º 4 do Ponto I, 2.000 km2 > área geográfica afetada ≥ 1.500 km2)
≥ 4 horas	30.000 > n.º de assinantes ou de acessos afetados ≥ 10.000 (ou, nos termos da alínea e) do n.º 4 do Ponto I, 1.500 km2 > área geográfica afetada ≥ 1.000 km2)
≥ 6 horas	10.000 > n.º de assinantes ou de acessos afetados ≥ 5.000 (ou, nos termos da alínea e) do n.º 4 do Ponto I, 1.000 km2 > área geográfica afetada ≥ 500 km2)
≥ 8 horas	5.000 > n.º de assinantes ou de acessos afetados ≥ 1.000 (ou, nos termos da alínea e) do n.º 4 do Ponto I, 500 km2 > área geográfica afetada ≥ 100 km2)

b) De qualquer violação de segurança ou perda de integridade que afete a entrega aos Postos de Atendimento de Segurança Pública (Centros de Atendimento do 112), direta ou indiretamente, das chamadas para o número único de emergência europeu 112, bem como das chamadas para o número nacional de emergência 115, por um período igual ou superior a 15 minutos;

c) De qualquer violação de segurança ou perda de integridade recorrente, sempre que o impacte acumulado das suas ocorrências num período de quatro semanas preencha uma das condições previstas nas alíneas anteriores;

d) De qualquer violação de segurança ou perda de integridade que se verifique numa data em que seja particularmente relevante o normal e contínuo funcionamento das redes e serviços, nos termos previstos no número 5 deste Ponto I, desde que:

   i) tenha uma duração igual ou superior a uma hora; e

   ii) afete um número de assinantes ou de acessos igual ou superior a 1.000 ou, nos termos da alínea e) do número 4 deste Ponto I, uma área geográfica igual ou superior a 100 km2;

e) De qualquer violação de segurança ou perda de integridade que impacte no funcionamento de todas as redes e serviços oferecidos por uma empresa na totalidade do território de uma ilha das Regiões Autónomas dos Açores ou da

Madeira, desde que tenha uma duração igual ou superior a 30 minutos, independentemente do número de assinantes ou de acessos afetados e da área geográfica afetada;

f) De qualquer violação de segurança ou perda de integridade, detetada pelas empresas ou a estas comunicada pelas entidades clientes, que impacte no funcionamento das redes e serviços através dos quais sejam prestados serviços relevantes à sociedade e aos cidadãos, por parte de entidades públicas ou privadas, de âmbito nacional ou regional, previstas no número 6 deste Ponto I, desde que tenha uma duração igual ou superior a 30 minutos; e

g) De qualquer violação de segurança ou perda de integridade cujo impacte acumulado sobre um conjunto de empresas que se encontrem nas condições previstas no n.º 2 do artigo 3.º da Lei n.º 19/2012, de 8 de maio, preencha uma das condições previstas na alínea a) e, na parte que remete para esta alínea, na alínea c), ambas do presente número 3.

4. Para efeitos do disposto no número anterior:

a) O impacte de uma violação de segurança ou perda de integridade deve ser aferido por referência a todas as redes e a todos os serviços de uma empresa que sejam afetados pela mesma;

b) O número de assinantes ou de acessos afetados por uma violação de segurança ou perda de integridade corresponde à soma do número de assinantes ou de acessos que são afetados pela mesma nas várias redes e serviços;

c) O número de assinantes de um serviço que seja suportado noutro serviço só será contabilizado quando o serviço de suporte não seja afetado;

d) O número de assinantes ou de acessos afetados corresponde ao número de assinantes ou de acessos que sejam abrangidos pela violação de segurança ou perda de integridade ou, na impossibilidade da sua determinação, a uma estimativa baseada nos elementos estatísticos detidos pela empresa; e

e) O critério relativo à área geográfica afetada só deve ser aplicado caso o critério relativo ao número de assinantes ou de acessos afetados seja inaplicável ou, no caso concreto, fundamentadamente impossível de determinar ou estimar.

5. Para os efeitos previstos na alínea d) do número 3 do presente Ponto I e sem prejuízo da identificação pelo ICP-ANACOM de outras datas, devidamente notificadas às empresas com uma antecedência mínima de cinco dias úteis, considera-se como datas relevantes as seguintes:

a) dia de eleições nacionais (legislativas, presidenciais, europeias ou autárquicas);

b) dia de referendos nacionais;

c) dia de exercício nacional de redes ou serviços de comunicações eletrónicas, ao abrigo do disposto na alínea c) do artigo 54.º-D da Lei das Comunicações Eletrónicas; e

d) dia de eleições regionais, no que respeita a violações de segurança ou perdas de integridade ocorridas na região em causa.

6. Para os efeitos previstos na alínea f) do número 3 do presente Ponto I e sem prejuízo da identificação pelo ICP-ANACOM de outras entidades, devidamente notificadas às empresas com uma antecedência mínima de cinco dias úteis, considera-se como entidade relevante o SIRESP – Sistema Integrado de Redes de Emergência e Segurança de Portugal.

II. Formato e Procedimentos

1. Por cada violação de segurança ou perda de integridade que deva ser objeto de notificação ao abrigo do disposto no Ponto I, as empresas devem submeter ao ICP-ANACOM:

a) uma notificação inicial, nos termos dos números 4 e 5 deste Ponto II;

b) uma notificação final, nos termos do número 8 e 9 deste Ponto II; e

c) sempre que exigida, em conformidade com o disposto no número 6 deste Ponto II, uma notificação de fim de violação de segurança ou perda de integridade com impacte significativo, nos termos dos números 6 e 7 deste Ponto II.

2. Na circunstância prevista na alínea c) do número 3 do Ponto I, as empresas apenas devem submeter ao ICP-ANACOM uma notificação final nos termos previstos nos números 8 e 9 deste Ponto II, com as devidas adaptações.

3. Na circunstância prevista na alínea g) do número 3 do Ponto I, pode ser dirigida ao ICP-ANACOM uma única série de notificações, nos termos previstos no número 1 do presente Ponto II, desde que as mesmas:

a) abranjam todo o impacte da violação de segurança ou perda de integridade; e

b) sejam apresentadas em representação de todas as empresas.

4. A notificação inicial deve ser enviada logo que seja possível e desde que a empresa possa concluir que existe ou existirá impacte significativo, até uma hora após a verificação da circunstância prevista no Ponto I que, no caso concreto, determinou a obrigação de notificação, devendo a empresa, sem prejuízo do cumprimento deste prazo, dar prioridade à mitigação e à resolução da violação de segurança ou perda de integridade.

5. A notificação prevista no número anterior deve incluir a seguinte informação:

a) Nome, número de telefone e endereço de correio eletrónico de um representante da empresa, para efeito de um eventual contacto por parte do ICP-ANACOM;
b) Data e hora em que a violação de segurança ou perda de integridade assumiu o impacte significativo ou, em caso de impossibilidade de a determinar, da sua deteção;
c) Data e hora em que a violação de segurança ou perda de integridade perdeu o impacte significativo ou, caso o mesmo se mantenha, o prazo estimado para a sua perda;

d) Breve descrição da violação de segurança ou perda de integridade, incluindo a indicação da categoria da causa raiz e, na medida do possível, o seu detalhe;

e) Estimativa possível do seu impacte, em termos de:

   i) redes e serviços afetados;

   ii) acesso aos serviços de emergência;

   iii) número de assinantes ou de acessos afetados;

   iv) área geográfica afetada, em km2; e

f) Observações.

6. Após a perda de impacte significativo da violação de segurança ou da perda de integridade e sempre que a mesma não tenha já sido comunicada na notificação inicial, as empresas devem submeter ao ICP-ANACOM, logo que possível, dentro do prazo máximo de duas horas após aquela ter ocorrido, uma notificação de fim de violação de segurança ou perda de integridade com impacte significativo.

7. A notificação referida no número anterior deve, na medida do possível, incluir a seguinte informação:

a) Atualização da informação transmitida na notificação inicial; e

b) Breve descrição das medidas adotadas para a resolução da violação de segurança ou perda de integridade.

8. A notificação final deve ser enviada no prazo de vinte dias úteis a contar do momento em que a violação de segurança ou perda de integridade deixou de assumir um impacte significativo.

9. A notificação prevista no número anterior deve incluir a seguinte informação:

a) Data e hora em que a violação de segurança ou perda de integridade assumiu o impacte significativo ou, em caso de impossibilidade de a determinar, da sua deteção;

b) Data e hora em que a violação de segurança ou perda de integridade perdeu o impacte significativo;

c) Data e hora do início ou, em caso de impossibilidade de o determinar, da deteção da violação de segurança ou perda de integridade e data e hora do respetivo fim, caso sejam diferentes das datas e horas transmitidas, respetivamente, ao abrigo das alíneas a) e b);

d) Impacte da violação de segurança ou perda de integridade em termos de:

   i) Redes (incluindo as interligações nacionais e internacionais) e respetivas infraestruturas (incluindo sistemas) e serviços afetados;

   ii) Acesso aos serviços de emergência pelo número único de emergência europeu 112 (incluindo o acesso pelo número nacional de emergência 115);

   iii) Número de assinantes ou de acessos afetados, por rede ou serviço;

iv) Percentagem do número de assinantes ou de acessos afetados em relação ao total de assinantes ou de acessos, por rede ou serviço; e

v) Área geográfica afetada, em km2;

e) Descrição da violação de segurança ou perda de integridade, com indicação da categoria da causa raiz e o respetivo detalhe;

f) Indicação das medidas adotadas para mitigar a violação de segurança ou perda de integridade;

g) Indicação das medidas adotadas para a resolução da violação de segurança ou perda de integridade, incluindo, no caso de violações de segurança ou perdas de integridade com tempos de restauração parciais, a cronologia e o detalhe das etapas de restauração;

h) Indicação das medidas adotadas e/ou planeadas para impedir ou minimizar a ocorrência de violações de segurança ou perdas de integridade similares no futuro (no âmbito do planeamento e/ou da exploração, do plano de contingência, dos acordos de interligação, dos acordos de níveis de serviços e de outras áreas pertinentes) e da data em que as mesmas foram ou serão tornadas efetivas;

i) Quando seja o caso, a informação disponibilizada ao público relativamente à violação de segurança ou perda de integridade, incluindo eventuais atualizações da mesma, bem como a data e a hora dessas comunicações;

j) Outra informação relevante; e

k) Observações.

10. Para os efeitos do disposto nos números 5, 7 e 9 deste Ponto II, as violações de segurança ou perdas de integridade podem ter as seguintes categorias de causas raiz:

a) Acidente/Desastre natural;

b) Erro humano;

c) Ataque malicioso;

d) Falha de *hardware/software*; ou

e) Falha no fornecimento de bens ou serviços por entidade externa.

11. A informação incluída nas notificações previstas neste Ponto II relativamente ao número de assinantes ou de acessos deve, sempre que possível, obedecer às definições fixadas no âmbito das obrigações de entrega de informação periódica ao ICP-ANACOM.

12. As notificações previstas neste Ponto II devem ser realizadas através dos seguintes meios:

a) no que respeita à notificação inicial e à notificação de fim de violação de segurança ou perda de integridade com impacte significativo, através do correio eletrónico notifica@anacom.pt e do número de telefone 214340899; e

b) no que respeita à notificação final, através de entrega em mão ou de correio registado.

13. As empresas cujas redes ou serviços sejam impactados no seu funcionamento pela mesma violação de segurança ou perda de integridade, devem cooperar entre si para a correta deteção e avaliação de impacte dessa violação de segurança ou perda de integridade e, no caso previsto na alínea g) do número 3 do Ponto I, para a respetiva notificação.

14. Tendo em vista o cabal cumprimento do disposto neste Anexo A, cabe às empresas implementar todos os meios e os procedimentos necessários à deteção, à avaliação do impacte e à notificação das violações de segurança ou perdas de integridade que preencham as circunstâncias previstas no Ponto I.

III. Entrada em vigor e disposição transitória

1. As empresas devem implementar as medidas necessárias ao cumprimento do disposto no presente Anexo A até ao dia 12 de junho de 2014, sem prejuízo do disposto no número seguinte.

2. As empresas devem remeter ao ICP-ANACOM, com base nos dados disponíveis e tendo por referência as circunstâncias previstas no Ponto I deste Anexo A e os requisitos exigidos para a notificação final no número 9 do Ponto II:

a) um relatório relativo ao período decorrido entre 1 de janeiro de 2013 e a data de aprovação desta decisão, a ser remetido até ao dia 12 de janeiro de 2014; e

seis relatórios mensais, de forma a abranger todo o período previsto no número 1 deste Ponto III, cada um deles a ser remetido no prazo de um mês a contar do final do período a que se refere.

ANEXO B ao SPD

- A **Cabovisão** considera não existir base legal para a obrigação imposta pelo ICP-ANACOM, e classifica-a de desproporcional, propondo que caso o ICP-ANACOM mantenha o previsto no SPD, reveja os patamares para níveis menos exigentes.

  Considera excessiva a divulgação na página eletrónica da empresa e pelo período de 6 meses, bastando na sua opinião o contacto telefónico abrangendo o IVR, bem como o prazo proposto, que deverá ser de 2 dias.

  Reafirmando o seu desacordo de princípio com a matéria, entende que deve ser considerado um prazo mínimo de implementação de 6 meses.
- Os **CTT** consideram que a divulgação a um público alargado e que não procura a informação poderá dar azo a um certo *"alarmismo"*, pelo que se deveria aferir a utilidade desta medida, e que o ICP-ANACOM deveria seguir a prática internacional de determinar caso a caso quais os incidentes de segurança a divulgar.

  Consideram que deveria apenas ser dado um contacto para o público procurar a informação, e entendem como razoável a informação ficar disponível pelo período de um (1) mês.

  Por último classificam de inexequível o prazo de 30 dias para a entrada em vigor.
- O **Grupo ONI** entende que a divulgação ao público poderá causar situações de *"alarmismo"* e eventuais ataques maliciosos devido à divulgação de vulnerabilidades, devendo ser assim limitada para minimizar riscos acrescidos.

  Discorda da manutenção de histórico nas páginas *web* das empresas, e sugere prazos de divulgação de 48 horas após determinação do ICP-ANACOM.

  A manter-se o disposto no SPD, entende que a manutenção da informação na página *web* deve ser de 5 dias úteis, e os prazos de entrada em vigor e disposição transitória alterados respetivamente para 6 e 5 meses.
- A **Optimus** também refere a possibilidade de, ao se revelar falhas de rede ou vulnerabilidades, poder-se estar a causar mais prejuízo do que benefício.

  Considera o prazo de uma hora irrealista, sugerindo 4 horas úteis após a deteção do incidente de segurança e a determinação do regulador e a sua devida comunicação à empresa.

Não concorda com a disponibilização na página eletrónica e, em especial, com a manutenção por 6 meses, e considera que a informação a disponibilizar deverá ser esclarecedora mas com o grau de detalhe adequado em função de uma análise custo/benefício em cada situação.

Faz proposta com base na tabela já transposta atrás, sendo a divulgação após 4 horas úteis e só após decisão do ICP-ANACOM.

O prazo de implementação deverá ser de, no mínimo, 6 meses.

- O **Grupo PT** refere que *"de forma a evitar um clima de desconfiança generalizada em relação aos operadores, a notificação aos clientes apenas deveria ser imposta quando precisamente, exista um risco real do incidente provocar danos e quando tal notificação apresente vantagens reais para os clientes"*.

  Considera que deve ser dada aos operadores alguma margem de manobra ou então ficar estabelecido que apenas estão sujeitos os incidentes graves que afetem o 112.

  Requer clarificação quanto à obrigatoriedade de contacto telefónico específico e entende que os meios deverão ser determinados caso a caso face ao tipo de incidente e o seu nível de criticidade.

  Entende que o prazo para a divulgação da informação ao público é *"bastante exigente"*, e que a manutenção da mesma na página *web* por 6 meses é *"absolutamente excessiva"*.

  Por fim considera que o prazo de entrada em vigor e da medida transitória deve ser de, no mínimo, 6 meses.

- A **Vodafone I.I.C. [Início de Informação Confidencial]**
  F.I.C. [Fim de Informação Confidencial]

- A **APRITEL** considera que, no limite, só *"determinados incidentes graves, que afetem o acesso ao 112, sejam abrangidos pela determinação prévia de interesse público"*.

  Refere igualmente eventual *"alarmismo"* desnecessário e que *"poderá haver clientes que são notificados de situações relativas a serviços que nem sequer usam ou que usam muito pontualmente"*, e que tal *"pode ainda contribuir para a descredibilização dos serviços de comunicações perante o público"*.

  Releva igualmente questões de exposição de vulnerabilidades, que a indicação do prazo expectável de resolução poderá *"potenciar situações de abuso por clientes"*, e que o prazo para divulgação é irrealista.

Considera que a decisão deverá entrar em vigor no prazo de 6 meses.

- O **GRM**, dadas as especificidades próprias das regiões autónomas, considera que também deveriam ser objeto de divulgação pública os incidentes de segurança a que se refere o ponto iv. da alínea c) do n.º I do ANEXO A ao SPD.

  Por outro lado considera que não deveriam ser objeto de divulgação pública *"ataques informáticos que atinjam empresas ou organismos governamentais"*.

ENTENDIMENTO DO ICP-ANACOM

De seguida, apresenta-se os fundamentos que suportam a versão final do Anexo B, destacando-se, antes de mais e no essencial, as seguintes alterações:

- Eliminação dos patamares de menor impacte quanto ao número de assinantes ou de acesso afetados (ou de área geográfica afetada);
- Eliminação da obrigação de disponibilização de um contacto telefónico;
- Fixação do prazo de divulgação em horas úteis; e
- Alargamento do prazo de entrada em vigor para um período correspondente a seis meses.

1. Em primeiro lugar importa esclarecer e relevar que as condições originalmente fixadas no SPD para a obrigação de divulgação ao público de violações de segurança ou perdas de integridade correspondiam exclusivamente às circunstâncias previstas na anterior alínea a) do Ponto I do Anexo A do SPD, não abrangendo, portanto, qualquer das outras alíneas desse Ponto.
2. Atente-se nas disposições que, sobre toda esta matéria, constam no capítulo 3 do regulamento da ARN finlandesa FICORA, e que de algum modo está em linha com o que defendemos.
3. Quer o Grupo PT quer a APRITEL colocam a hipótese de se divulgar ao público apenas a informação sobre os incidentes de segurança com os centros de atendimento do 112;

   O ICP-ANACOM considera que, neste caso específico, deve o ICP-ANACOM avaliar a situação se e quando tal acontecer, pois desde logo importa ter presente que os centros de atendimento 112 são da responsabilidade do Ministério da Administração Interna.
4. Ao contrário do referido eventual *"alarmismo"* e *"descredibilização dos serviços de comunicações perante o público"* o ICP-ANACOM, para lá do antes referido, entende o seguinte:
   a. Um dos racionais da Diretiva Quadro e da LCE em matéria de segurança e integridade das redes e serviços é, como já foi atrás referido, a transparência;
   b. Eventual *"alarmismo"*, *"descredibilização"*, ou até especulação, poderia decorrer da divulgação ao público de informação não fidedigna, não devidamente tratada por quem a detém em primeira mão, e que assim tem a possibilidade, e o dever, de informar devidamente o público;
   c. Obviamente que não será, em princípio, de interesse público conhecer eventuais vulnerabilidades que possam ou tenham sido exploradas, e nunca tal esteve em *"cima da mesa"*;
   d. Consideramos que é de interesse público conhecer-se quanto antes a informação relativa a um incidente de segurança que teve um impacte significativo nos utilizadores e que, como tal, não é possível nos dias de hoje esconder; será em nosso

entender menos alarmista, menos especulativo, e dará uma melhor imagem das empresas, serem as próprias empresas a darem a informação em tempo útil sobre esse incidente de segurança;

5. Por outro lado e ao contrário do que foi referido por várias empresas, a informação sobre um determinado incidente de segurança não interessa apenas, na maior parte das vezes, aos assinantes diretamente afetados, mas também a todos os outros utilizadores que ficam então impedidos de comunicar com aqueles.
6. No que respeita à divulgação dos incidentes de segurança, ocorridos nas Regiões Autónomas, de acordo com o disposto no item iv) da alínea c) do Ponto I do Anexo A do SPD, considera-se que seria desproporcionado, sendo alvo de análise por parte do ICP-ANACOM quando da sua eventual ocorrência.
7. Quanto a acautelar a divulgação pública de *"ataques informáticos que atinjam empresas ou organismos governamentais"*, releve-se que desde logo não é objetivo divulgar informação ao público, no âmbito da presente matéria, relativa a incidentes de segurança que impactem especificamente neste ou naquele utilizador final.
8. Ponderados os comentários recebidos quanto à fixação da dimensão do impacte das violações de segurança ou perdas de integridade para efeitos da determinação da respetiva divulgação ao público, considera-se que, neste momento, só se devem considerar as violações de segurança ou perdas de integridade de maior impacte, pelo que, nos termos que ficam definidos nos n.^{os} 2 e 3 do Ponto I do Anexo B, se eliminam os dois patamares de menor impacte quanto ao número de assinantes ou de acesso afetados (ou de área geográfica afetada) antes previstos no SPD.
9. Para além disso e para efeitos da interpretação e da aplicação das circunstâncias previstas no n.º 2 do Ponto I do Anexo B, transpõem-se, para o n.º 3 deste Ponto, regras idênticas àquelas constantes do n.º 4 do Ponto I do Anexo A.
10. No que respeita ao conteúdo da informação a disponibilizar, as empresas devem ter procedimentos adequados de comunicação que não ponham em causa a segurança das suas redes e serviços;

O conteúdo da informação a divulgar acerca das violações de segurança ou perdas de integridade deve ser, conforme fica previsto na alínea a) do n.º 1 do Ponto II do Anexo B, claro, acessível e tão preciso quanto possível, incluindo, entre outros elementos considerados relevantes, a indicação das redes e serviços afetados e o prazo expectável de resolução ou, quando for o caso, a data de resolução.

No que se refere aos prazos, não se entende a preocupação da APRITEL com a divulgação do prazo expectável de resolução por *"potenciar situações de abuso por clientes"*; como não concretizam, e lembrando que o público não terá em princípio conhecimento de eventuais incidentes de segurança que não impactem o normal funcionamento das redes e serviços percecionado pelo utilizador, não se entende o alcance do referido pela APRITEL.

11. O meio através do qual as empresas devem disponibilizar a informação ao público deve ser, no mínimo, os respetivos sítios na Internet que utilizam no seu relacionamento com os utilizadores das suas redes e dos seus serviços, através de uma hiperligação imediatamente visível e identificável na primeira página do sítio sem necessidade do uso da barra elevatória, conforme fica previsto na alínea b) do n.º 1 do Ponto II do Anexo B.

    Neste ponto e ao invés do que previámos no SPD, e do que a FICORA adotou, entende-se agora que não deve ser utilizado contacto telefónico específico para o público averiguar acerca de determinado incidente de segurança, pois este não será o meio mais indicado para divulgar informação; considera-se no entanto que as empresas, se contactadas sobre a ocorrência através desse canal, não poderão deixar de manter os seus assinantes devidamente informados quanto a incidentes de segurança que os afetem, de acordo com os deveres gerais de informação que resultam da lei, do contrato e do princípio da boa-fé.

12. Por outro lado fomos sensíveis a alguns argumentos como a distribuição horária ao longo das 24 horas, quer quanto ao custo do trabalho quer quanto à relevância da divulgação da informação (e que pode sempre vir a ser alterado se, perante casos concretos, o ICP-ANACOM assim o vier a determinar), e a necessidade de mais tempo para tratar a informação de modo à mesma ser esclarecedora, e assim:

a. Entende o ICP-ANACOM que, conforme agora fica disposto na alínea c) do n.º 1 do Ponto II do Anexo B, a informação deve ser divulgada logo que possível, no prazo máximo de quatro horas úteis após o termo do prazo de notificação inicial ao ICP-ANACOM da violação de segurança ou perda de integridade previsto no Ponto II do Anexo A, considerando-se como horas úteis, para o efeito, as horas decorridas entre as nove e as dezanove horas de um dia útil;
b. Num exemplo, se o prazo de notificação inicial ao ICP-ANACOM da violação de segurança ou perda de integridade terminar às 22 horas de um determinado dia, a informação relativa à mesma deve ser disponibilizada ao público até às 13 horas do dia útil seguinte;
c. Nos termos previstos nas alíneas d) e e) do mesmo n.º 1 do Ponto II do Anexo B, as empresas devem atualizar a informação sempre que se verifique alguma alteração significativa e logo após o fim da violação de segurança ou perda de integridade, devendo ainda a informação disponibilizada através da Internet manter-se acessível ao público durante o período de um mês a contar da data do fim da violação de segurança ou perda de integridade, à semelhança do que a FICORA adotou.

13. Nos termos do disposto no n.º 2 do ponto II do Anexo B, as empresas devem comunicar, quando do início da atividade ou quando da alteração dos mesmos, os endereços URL das suas páginas da Internet onde, para efeitos do disposto na alínea b) do n.º 1, disponibilizam a informação ao público.
14. Nos termos do disposto no novo n.º 3 do Ponto II do Anexo B e tendo em vista o cabal cumprimento do disposto neste Anexo B, determina-se que cabe às empresas implementar todos os meios e os procedimentos necessários à deteção, à avaliação do impacte e à divulgação das violações de segurança ou perdas de integridade que preencham as circunstâncias previstas no Ponto I do mesmo Anexo B.
15. Pelas razões já referidas e nos termos que ficam previstos no n.º 1 do Ponto III do Anexo B, o ICP-ANACOM entende que o prazo de entrada em vigor deve corresponder a um período de seis meses após a data

da decisão final. Para que o ICP-ANACOM seja, à partida, dotado da informação necessária a um acompanhamento do cumprimento desta decisão, prevê-se ainda no n.º 2 do mesmo Ponto III que, com uma antecedência mínima de 15 dias úteis relativamente ao termo do prazo de entrada em vigor, as empresas devem comunicar a esta Autoridade os endereços URL nos quais será disponibilizada ao público a informação relativa às violações de segurança ou perdas de integridade.

16. À semelhança do efetuado relativamente ao Anexo A da decisão, reformulou-se o Anexo B no sentido de lhe conferir maior precisão e clareza.

VERSÃO FINAL DO ANEXO B:

Divulgação ao público por parte das empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público, de violações de segurança ou perdas de integridade ocorridas nas suas redes e serviços

I. Condições

1. Nos termos do disposto na alínea b) do artigo 54.º-E da Lei n.º 5/2004, de 10 de fevereiro, alterada e republicada pela Lei n.º 51/2011, de 13 de setembro (doravante, a «Lei das Comunicações Eletrónicas»), compete ao ICP – Autoridade Nacional de Comunicações (ICP-ANACOM) determinar às empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público (doravante, as «empresas») que, pelos meios adequados, informem o público das violações de segurança ou das perdas de integridade da rede, quando tal seja considerado pelo ICP-ANACOM como de interesse público.

2. O ICP-ANACOM determina que é de interesse público que as empresas informem o público de qualquer violação de segurança ou perda de integridade cujo impacte no funcionamento das suas redes e serviços se inclua num dos seguintes patamares:

Duração, e	**Número de assinantes ou de acessos afetados (ou, nos termos da alínea e) do n.º 3 do Ponto I, área geográfica afetada)**
≥ 30 minutos	n.º de assinantes ou de acessos afetados ≥ 500.000 (ou, nos termos da alínea e) do n.º 3 do Ponto I, área geográfica afetada ≥ 3.000 km2)
≥ 1 hora	500.000 > n.º de assinantes ou de acessos afetados ≥ 100.000 (ou, nos termos da alínea e) do n.º 3 do Ponto I, 3.000 km2 > área geográfica afetada ≥ 2.000 km2)
≥ 2 horas	100.000 > n.º de assinantes ou de acessos afetados ≥ 30.000 (ou, nos termos da alínea e) do n.º 3 do Ponto I, 2.000 km2 > área geográfica afetada ≥ 1.500 km2)
≥ 4 horas	30.000 > n.º de assinantes ou de acessos afetados ≥ 10.000 (ou, nos termos da alínea e) do n.º 3 do Ponto I, 1.500 km2 > área geográfica afetada ≥ 1.000 km2)

3. Para efeitos do disposto no número anterior:

a) O impacte de uma violação de segurança ou perda de integridade deve ser aferido por referência a todas as redes e a todos os serviços de uma empresa que sejam afetados pela mesma;
b) O número de assinantes ou de acessos afetados por uma violação de segurança ou perda de integridade corresponde à soma do número de assinantes ou de acessos que são afetados pela mesma nas várias redes e serviços;
c) O número de assinantes de um serviço que seja suportado noutro serviço só será contabilizado quando o serviço de suporte não seja afetado;
d) O número de assinantes ou de acessos afetados corresponde ao número de assinantes ou de acessos que sejam abrangidos pela violação de segurança ou perda de integridade ou, na impossibilidade da sua determinação, a uma estimativa baseada nos elementos estatísticos detidos pela empresa; e
e) O critério relativo à área geográfica afetada só deve ser aplicado caso o critério relativo ao número de assinantes ou de acessos afetados seja inaplicável ou, no caso concreto, fundamentadamente impossível de determinar ou estimar.

4. O disposto no presente Anexo B não prejudica que, em circunstâncias não previstas no número 2 deste Ponto I e sempre que o também considere de interesse público, o ICP-ANACOM possa, ao abrigo do disposto na alínea b) do artigo 54.º-E da Lei das Comunicações Eletrónicas, determinar às empresas que informem o público de violações de segurança ou perdas de integridade ocorridas nas suas redes e serviços.

II. Conteúdo, meios e prazos de divulgação

1. Na informação ao público das violações de segurança ou das perdas de integridade a que se refere o Ponto I, as empresas devem:

a) Assegurar que o conteúdo da informação seja claro, acessível e tão preciso quanto possível e inclua, entre outros elementos considerados relevantes:

i) A indicação das redes e serviços afetados; e

ii) O prazo expectável de resolução ou, quando for o caso, a data de resolução;

b) Disponibilizar a informação, no mínimo, nos respetivos sítios na Internet que utilizam no seu relacionamento com os utilizadores, através de uma hiperligação

imediatamente visível e identificável na primeira página do sítio sem necessidade do uso da barra elevatória;

c) Disponibilizar a informação logo que possível, no prazo máximo de quatro horas úteis após o termo do prazo de notificação inicial ao ICP-ANACOM[23], considerando-se como horas úteis, para o efeito, as horas decorridas entre as nove e as dezanove horas de um dia útil;

d) Atualizar a informação sempre que se verifique alguma alteração significativa e logo após o fim da violação de segurança ou perda de integridade; e

e) Manter a informação disponibilizada através da Internet acessível ao público, nas mesmas localizações referidas na alínea b), durante o período de um mês a contar da data do fim da violação de segurança ou perda de integridade.

2. As empresas devem comunicar ao ICP-ANACOM, logo que iniciem a sua atividade, os endereços URL[24] das páginas na Internet nas quais, para efeitos do disposto na alínea b) do número anterior, procederão à divulgação ao público das violações de segurança ou perdas de integridade ocorridas nas suas redes e serviços, bem como qualquer alteração posterior dos mesmos com uma antecedência mínima de 5 dias úteis relativamente à sua execução.

3. Tendo em vista o cabal cumprimento do disposto neste Anexo B, cabe às empresas implementar todos os meios e os procedimentos necessários à deteção, à avaliação do impacte e à divulgação das violações de segurança ou perdas de integridade que preencham as circunstâncias previstas no Ponto I.

III. Entrada em vigor e disposição transitória

1. As empresas devem implementar as medidas necessárias ao cumprimento do disposto no presente Anexo B até ao dia 12 de junho de 2014.

2. As empresas devem comunicar ao ICP-ANACOM, com uma antecedência mínima de 15 dias úteis relativamente ao termo do prazo previsto no número anterior, os endereços URL referidos no número 2 do Ponto II.

---

[23] Em conformidade com o disposto no Ponto II do Anexo A.

[24] *Uniform Resource Locator*.