**CONSULTA PÚBLICA SOBRE SEGURANÇA E INTEGRIDADE DAS REDES E SERVIÇOS DE COMUNICAÇÕES ELECTRÓNICAS:**

Na sequência da consulta pública lançada pelo ICP-ANACOM no passado dia 30.12.2011, quanto aos Projectos de Decisão relativos às circunstâncias, formato e procedimentos aplicáveis à comunicação das violações de segurança ou das perdas de integridade com impacte significativo no funcionamento das redes ou serviços de comunicações electrónicas acessíveis ao público e, bem assim, às condições em que o ICP-ANACOM considera existir um interesse público na divulgação dessa informação ao público, vem a Cabovisão – Televisão por Cabo, S.A. (Cabovisão) apresentar os seus comentários.

## I. COMENTÁRIOS GERAIS

1. 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**. Esta empresa concorda inteiramente com o Regulador considerando que só assim se garante a coerência na abordagem à matéria, e aproveita para reiterar o seu empenho em garantir a segurança e o adequado funcionamento e disponibilidade das suas redes e serviços de comunicações electrónicas.

2. A **Cabovisão confere uma importância primordial à protecção da integridade e segurança** das redes e serviços de comunicações electrónicas, visível nos avultados investimentos que tem feito nesta matéria, tendo implementado com sucesso diversos procedimentos internos de garantia e de prevenção de incidentes de segurança e participado em diferentes mecanismos de cooperação sectorial, como seja o CSIRT. Tem ainda colaborado prontamente com as Autoridades competentes, sendo de referir a implementação do Sistema ePrivacy em total conformidade com o normativo sobre a retenção de dados para efeitos de partilha com a Justiça, que importou esforços de investimento substanciais.

3. Sem prejuízo do exposto, a Cabovisão entende que é **fundamental que o ICP-ANACOM revisite determinados aspectos contemplados no Projecto de Decisão** relativo à comunicação de incidentes de segurança (Projecto de Decisão I), sob pena de adoptar uma posição demasiado exigente, sem paralelo nas posições assumidas pela ENISA[1] e pela OFCOM[2], que coloca **obrigações desproporcionais aos operadores, exigindo-lhes avultados esforços de investimento e de adopção de novos procedimentos organizacionais, sem que na prática isso se traduza numa real contribuição para o reforço do nível de segurança das comunicações electrónicas**.

4. Em concreto, a Cabovisão entende que o ICP-ANACOM deve **delimitar claramente, e desde logo, o que são "incidentes de segurança" notificáveis**, e fazê-lo nos exactos moldes em que o fez a ENISA, estabelecendo que estão em causa incidentes e violações de segurança que impliquem a *interrupção* da prestação de serviços de comunicações electrónicas.

5. Deve clarificar-se igualmente que **a obrigação de notificação não abrange os casos de manutenções ou melhorias de rede programadas**. Trata-se de operações que constituem actividades correntes no âmbito dos processos habituais de um operador de comunicações electrónicas, para manutenção e melhoria das suas infra-estruturas e, na medida em que não são considerados incidentes pelos operadores, não o devem ser pelo ICP-ANACOM.

6. Além disso, o ICP-ANACOM deve **flexibilizar os critérios que qualificam um "incidente de segurança" como tendo um "impacte significativo"**, nomeadamente especificando os serviços elegíveis para efeitos de notificação, distinguido a necessidade de notificação por nível de criticidade de serviço, bem como relaxando os critérios que despoletam a obrigação de notificação, quer quanto à duração do incidente, ao número de assinantes afectados e ao critério geográfico (que não é passível de ser contabilizado), quer também quanto aos prazos de notificação, que são manifestamente insuficientes.

7. Em especial, a Cabovisão solicita ao ICP-ANACOM que, **em linha com o entendimento da OFCOM, procure minimizar tanto quanto possível o impacto que estas obrigações de notificação possam ter sobre os operadores de menor dimensão**, relativamente aos

[1] Linhas de orientação da ENISA sobre as notificações de violações de segurança e de perdas de integridade " Technical Guideline on Reporting Incidents - Article13a Implementation", de Dezembro de 2011

[2] "OFCOM Guidance on security requirements in the revised Communications Act 2003 – Implementing the revised EU Framework", de 11 de Maio de 2011

quais o esforço de adaptação implicará, necessariamente, um custo muito maior – ainda que procurando garantir que os incidentes mais significativos sejam reportados.[3] É essencial que o *approach* final adoptado tenha em conta estas considerações de proporcionalidade que, no contexto económico actual, ganham uma especial acuidade.

8. E isto é ainda mais **crucial tendo em conta as elevadíssimas coimas** potencialmente aplicáveis ao incumprimento da obrigação de notificação de incidentes de segurança ao Regulador, que podem ir **até 1M€** no caso de empresas que, para efeitos dos critérios legais", sejam consideradas 'grandes empresas'.

9. Por fim, é **imprescindível que o ICP-ANACOM preveja um prazo mais alargado** para a implementação das eventuais medidas necessárias para garantir a notificação de incidentes de segurança ao Regulador. O prazo de 30 dias é manifestamente insuficiente, em especial quando o ICP-ANACOM é o primeiro a reconhecer a novidade do tema, tanto a nível nacional como europeu, bem como quando se tem em conta as já referidas sanções contra-ordenacionais aplicáveis. No mínimo, o prazo a prever deverá corresponder a um **período de 6 meses**.

10. No que respeita ao **Projecto de Decisão relativo às condições em que o ICP-ANACOM considera existir um interesse público** na divulgação dessa informação ao público (Projecto de Decisão II), **a Cabovisão não está de acordo com a proposta do Regulador.**

11. **A Cabovisão entende que o ICP-ANACOM deve determinar, caso a caso, e face às características concretas de cada situação, quais os incidentes de segurança que revestem um interesse público que imponha a sua divulgação ao público em geral**. Não faz sentido impor de antemão aos operadores uma verdadeira obrigação de divulgar ao público, através dos seus websites e contactos telefónicos, um número tão alargado de incidentes – que podem nem ter especial gravidade ou impacto, na realidade.

12. Nem parece ser essa a *ratio* da alínea b) do artigo 54.º-E da Lei n.º 5/2004, de 10 de Fevereiro, na sua última redacção, cuja epígrafe dispõe que a informação ao público se trata de "obrigações de informação da ARN" que, eventualmente, pode determinar às empresas que o façam, quando o considere de interesse público.

[3] Com efeito, a OFCOM refere que "it is likely that complying with the new requirements will impose a greater cost on these providers [smaller providers], relative to their size", "where it does apply, the reporting process is intended to minimise the burden on providers as far as possible, while still ensuring that no significant incidents go unreported"

13. Esta disposição transpôs para o Direito Nacional o novo n.º 3 do artigo 13.º-A da Directiva 2002/21/CE que dispõe que "*a autoridade reguladora nacional em questão pode informar o público ou exigir que as empresas o façam, sempre que determine que* ***a revelação da violação*** *é do interesse público*." [4]

14. Ou seja, face a cada incidente concreto de *violação de segurança*, o ICP-ANACOM deve determinar se há um interesse público na sua revelação ao público.

15. Não se trata de algo que possa ser determinado previamente e, sobretudo, fazendo referência a elenco tão vasto de incidentes quanto os visados pelo Projecto de Decisão II.

16. Neste sentido, veja-se a posição que OFCOM se propõe adoptar nesta matéria, de deixar que a avaliação do interesse público na divulgação de um determinado incidente de segurança se faça perante cada caso concreto e respectivas circunstâncias.

17. Assim sendo, a decisão proposta, tal como está configurada – que estabelece *a priori* que é do interesse público que os operadores divulguem ao público todos os incidentes cujo impacte se inclua num dos critérios que despoletam a obrigação de notificação ao abrigo do Projecto de Decisão I –, ao impor às empresas uma verdadeira *obrigação* de divulgação geral de incidentes ao público, num prazo manifestamente inexequível, não deve ser admissível.

18. Além de não ter uma concreta base legal, não traz qualquer utilidade acrescida em termos de reforço de segurança de redes, implica custos significativos para os operadores, e pode ainda provocar reacções adversas nos utilizadores, bem como criar riscos de segurança evitáveis.

19. Com efeito, a Cabovisão já garante, através do seu sistema automático de atendimento, que os clientes que residem em áreas afectadas por violações de segurança e perdas de integridade da rede e dos serviços são devidamente informados destas situações, bem como do prazo previsto para a respectiva resolução.

[4] Novo n.º 3 do artigo 13.º-A da Directiva 2002/21/CE relativa a um quadro regulamentar comum para as redes e serviços de comunicações electrónicas (Directiva Quadro), alterada pela Directiva 2009/140/CE

20. Impor uma obrigação adicional em que os operadores tenham de divulgar, no mínimo, nos respectivos sítios da internet (em local de destaque) um leque alargado de incidentes de segurança – que podem nem revestir, na prática, interesse público – constitui uma intervenção demasiado intrusiva na esfera económica privada que deve ser evitada a todo o custo.

21. Além de que previsivelmente provocará congestionamentos na página de web dos operadores – o que desde logo tornaria a informação ininteligível, frustrando o objectivo que se visa cumprir, que é o de informar o público sobre incidentes de segurança graves.

22. E isto somado ao facto que, em caso de indisponibilidade dos Serviços (IP), os clientes dificilmente teriam acesso à página da Cabovisão, ou caso a falha seja interna e grave, o próprio *site* poderá estar indisponível.

23. Além disso, em termos de histórico, coloca-se também o tema do armazenamento e retenção dessa informação, o que tem custos e impactos operacionais que têm de ser contemplados e que podem ser relevantes.

24. A Cabovisão entende pois que o Regulador deve reanalisar a necessidade de adopção de um Projecto de Decisão desta natureza ou, caso entenda ser de manter, deve limitar ao máximo os casos previstos como sendo 'divulgáveis' por interesse público, restringindo-os aos casos relativos a incidentes realmente graves, como sejam os incidentes que afectem o acesso ao número único de emergência 112.

## II. PROJECTO DE DECISÃO RELATIVO ÀS CIRCUNSTÂNCIAS, FORMATO E PROCEDIMENTOS APLICÁVEIS À COMUNICAÇÃO DAS VIOLAÇÕES DE SEGURANÇA OU DAS PERDAS DE INTEGRIDADE COM IMPACTE SIGNIFICATIVO

### A. CIRCUNSTÂNCIAS

25. Sem prejuízo dos comentários introdutórios – como sejam, em especial, a necessidade de concretizar o conceito de "incidente de segurança" por referência à continuidade do serviço – a Cabovisão considera que os critérios que qualificam um incidente de segurança como tendo um impacto significativo devem ser alterados na linha do

estipulado nas orientações da ENISA[5] e, bem assim, tendo em conta os investimentos que estão associados à exigência de um número excessivo de notificações (em quantidade e conteúdo) para os operadores de menor dimensão.

26. Em concreto, quanto aos patamares de duração definidos, a Cabovisão considera injustificada a notificação de incidentes cujo impacto tenha uma duração inferior a 4 horas – que nem pela ENISA são considerados como incidentes significativos. Assim sendo, o patamar mínimo de duração deve iniciar-se nas 4 horas.

27. Mais, quando determinar o número de assinantes afectados, para a dita duração de 4 horas, o ICP-ANACOM deve fundamenta como determinou que esse patamar de assinantes afectados, em conjugação com a duração do incidente, importa um impacte significativo nas redes e serviços de comunicações electrónicas. A Cabovisão relembra que deverá sido tida em conta, tal como aconselha a ENISA, a expressão entre o número de assinantes afectados e o número total de utilizadores do serviço afectado.

28. Além disso, e à semelhança do que efectuou a ENISA, o ICP-ANACOM deve efectuar a distinção do tipo de serviço afectado por incidente. Da actual proposta do ICP-ANACOM não consta qualquer especificação dos serviços elegíveis para notificação, pelo que tudo indica que os operadores são obrigados a reportar ao Regulador incidentes de segurança que afectem quaisquer dos serviços prestados aos seus clientes – serviços de dados, televisão, telefonia, *vídeo on demand*, email, etc.

29. Assim, deve alterar-se a tabela constante do ponto I.a) para que passe a distinguir níveis de criticidade por serviço (não sendo de descurar que um incidente com uma dada duração que afecte um determinado número de utilizadores e que impacte apenas no serviço de dados não terá, necessariamente, a mesma relevância que um incidente nos serviços de voz).

30. Quanto ao patamar da área geográfica afectada, actualmente previsto na tabela constante do ponto I.a), devido à tecnologia, estrutura e tipologia da rede de serviços da

[5] Com efeito, a ENISA refere claramente nas suas Linhas de Orientação que, "*this document does not go into details about how the NRAs can design or implement the national incident reporting schemes but it does, by* ***providing a single definition of incident paramaters and thresholds****, provide a baseline for those national schemes*". (sublinhado nosso)

Cabovisão, é actualmente inviável para esta empresa efectuar verificação de impacto de incidentes com base na área geográfica afectada. Assim, para a Cabovisão, apenas é exequível contabilizar o impacto de incidentes segundo os indicadores de duração e número estimado de clientes afectados.

31. Relativamente ao ponto I.b), deve notar-se que o único cenário em que a Cabovisão ficaria impedida de entregar chamadas ao número único de emergência europeu seria devido a uma falha de interligação com a Portugal Telecom que afectasse os dois pontos de interligação actualmente existentes com esse operador. Caberia saber se, nestes casos, quando a *root cause* reside no operador Portugal Telecom, é proporcional que seja a Cabovisão a ser onerada com a obrigação de reportar o incidente.

32. Mas, ainda relativamente a este ponto, cumpre saber se, caso um dos pontos de interligação falhe mas o segundo não, não afectando a entrega de chamadas ao 112, mas podendo impedir que a chamada seja entregue no centro de atendimento mais próximo do cliente, ainda assim esta circunstância é considerada elegível para *reporting*.

33. No que diz respeito ao ponto I.c) (i), a Cabovisão chama a atenção para o facto de que é actualmente inviável contabilizar incidentes de segurança que isoladamente no tempo não têm impacte significativo mas que, caso se verifiquem repetidamente durante um período de um mês atingem, no seu impacto acumulado durante este período de tempo, um dos patamares definidos na tabela constante do ponto I.a).

34. Relativamente ao ponto I.c) (ii), a Cabovisão nota que não é possível prever que os operadores partilhem indicadores relativos a impactos de incidentes no sentido de verificar se o impacto acumulado é elegível a *reporting* de acordo com os patamares da tabela I.a).

35. Já quanto ao ponto I.c) (iii), para que seja exequível, é necessário que o ICP-ANACOM defina as datas ou eventos elegíveis. Caso contrário, será necessário que os operadores sejam notificados com antecedência relativamente a datas ou eventos especiais, para que possam contemplar esta medida extraordinária de *reporting*.

36. Finalmente, quanto ao ponto I.d), e à semelhança do comentário anterior, o ICP-ANACOM deve definir claramente a lista de assinantes contemplados nesta medida - organismos

governamentais ou regionais, ou outras entidades relevantes em termos de serviços à sociedade e aos cidadãos (e.g. SIRESP), em termos nacionais ou regionais.

**B. FORMATO E PROCEDIMENTOS**

37. Em termos de **formato previsto para a notificação de incidentes de segurança** ao ICP-ANACOM, a Cabovisão sublinha, desde já, que considera excessiva, desproporcional e desnecessária a submissão de duas a três notificações por incidente.

38. A obrigação de notificar o ICP-ANACOM, no mínimo, duas vezes por cada incidente constitui um custo que onera os operadores de forma desproporcional face à utilidade que o ICP-ANACOM daí retira.

39. No limite, um volume excessivo de notificações pode implicar o bloqueio do sistema ou a incapacidade de análise, não trazendo qualquer utilidade acrescida para a segurança de redes e serviços. Acresce que o ICP-ANACOM poderá não ter capacidade para analisar e tratar notificações enviadas em períodos não laborais e, mesmo que tenha, questiona-se a relevância de enviar as notificações nesses períodos. É de sublinhar que o envio de notificações ao ICP-ANACOM nesses períodos constitui para a Cabovisão um impacto em termos de custos e de gestão de recursos humanos não despiciendo, pelo que a sua necessidade deve ser devidamente fundamentada pelo Regulador.

40. Aliás, na sua decisão final, o ICP-ANACOM deve fundamentar claramente a necessidade de receber as notificações que exigir, bem como a informação solicitada (que, no Projecto de Decisão I, é demasiado extenso), explicando a utilização que fará dos relatórios.

41. Assim sendo, a Cabovisão considera que, ao contrário do proposto no Projecto de Decisão I, o ICP-ANACOM deve optar por seguir a orientação da OFCOM nesta matéria, e exigir apenas um relatório de notificação inicial e, eventualmente, caso o incidente em causa assim o justifique, solicitar um segundo relatório.

42. O primeiro relatório inicial deve ser o mais *lightweight* possível, por forma a minimizar o encargo imposto aos operadores, e deverá ser entregue dentro de poucos dias da ocorrência do incidente (se for um incidente que se considere *life affecting* – por afectar o acesso ao número 112, por exemplo –, poderá prever-se um prazo mais curto). Já o segundo relatório só deve ser exigido pelo ICP-ANACOM caso o incidente em causa assim

o justifique, por forma a permitir-lhe compreender melhor os contornos do incidente, quer durante a sua ocorrência, quer após a efectiva resolução. Também neste caso o conteúdo exigido deve ser propositadamente *high level* e breve.

43. Não se aceita o que propõe o Regulador quanto ao relatório final, de definir acções e *timings* para a implementação de acções correctivas no sentido de evitar reincidências. Trata-se de temas da vida interna das empresas que, na maior parte das vezes, implicam a tomada de decisões de investimento (em montantes significativos), que dificilmente se adequariam a quaisquer prazos de notificação impostos por uma entidade reguladora.

44. Quanto aos **prazos previstos para a submissão das notificações**, a Cabovisão considera que o prazo máximo de notificação de duas horas após a detecção do incidente de segurança especificado pelo Regulador é inviável, *tout court.*

45. A notificação deve ser feita num prazo máximo de 2 dias, por ser mais realista face aos condicionalismos de uma situação de incidentes, devendo este prazo ser contabilizado a partir do momento da detecção do incidente e não do seu início.

46. A Cabovisão regista, quanto a isto, o que refere o ICP-ANACOM, que a prioridade máxima deve ser dada à mitigação e resolução dos incidentes de segurança e, apenas depois, à compilação da informação quanto à causa provável, impacte e prazo expectável de restauração para informação ao público. Mas nota que, caso sejam impostos os prazos e as exigências de notificação ora propostos, certamente se assistirá a uma inversão de prioridades.

47. Quanto ao **modo de submissão das notificações**, a Cabovisão considera insuficiente a disponibilização de um único endereço de correio electrónico, não sendo prevista qualquer forma de os operadores certificarem-se que o *email* foi devidamente recebido pelo ICP-ANACOM, devendo prever-se um tempo de reacção (para acusação de recepção) pelo Regulador.

48. No que respeita à **cooperação entre as diferentes empresas**, a Cabovisão reitera que é inexequível que as empresas, cujas redes ou serviços sejam impactados no seu funcionamento por um mesmo incidente de segurança, cooperem entre si para a notificação desse incidente de segurança. Diferente será a cooperação para a correcta

detecção, avaliação de impacte e resolução do incidente de segurança, que os operadores já efectuam.

49. Já no que respeita às **causas de raiz**, por razões de segurança jurídica, deve estabelecer-se uma lista exaustiva de *root causes* elegíveis para gerar uma obrigação de *reporting* de incidente de segurança.

50. Finalmente, não é claro o significado da frase "os dados a incluir nas notificações relativamente ao impacte nos utilizadores deverão, sempre que possível, ser consonantes com os dados estatísticos disponibilizados trimestralmente ao ICP-ANACOM". Pede-se, assim, ao Regulador que clarifique.

### C. ENTRADA EM VIGOR

51. Conforme referido nos comentários introdutórios, a Cabovisão considera que o prazo de 30 dias para a implementação das eventuais medidas necessárias para garantir a notificação de incidentes de segurança ao Regulador é manifestamente insuficiente, não sendo aceitável.

52. A novidade do tema, os elevados encargos associados à implementação deste tipo de medidas por parte dos operadores – que terão de efectuar alterações que exigirão investimentos, alterações organizacionais, alterações de contratos de trabalho e outras medidas ainda não identificadas –, bem como as pesadas sanções contra-ordenacionais previstas para o incumprimento da obrigação de notificação, ditam que o ICP-ANACOM preveja um prazo mais alargado – no mínimo, de 6 meses.

## III. PROJECTO DE DECISÃO RELATIVO ÀS CONDIÇÕES EM QUE O ICP-ANACOM CONSIDERA EXISTIR UM INTERESSE PÚBLICO NA DIVULGAÇÃO DESSA INFORMAÇÃO AO PÚBLICO

### A. CONDIÇÕES

53. Conforme referido nos comentários gerais, a Cabovisão não concorda com a proposta do Regulador, entendendo que a avaliação do interesse público na divulgação de um determinado incidente de segurança se deve fazer perante cada caso concreto e respectivas circunstâncias.

54. Não só não é possível determinar, de antemão, se a revelação de um dado incidente (cujos contornos se desconhecem) é do interesse público, como – em conformidade com o referido nos comentários gerais – não existe qualquer base legal para o ICP-ANACOM impor aos operadores uma verdadeira obrigação de divulgar ao público, através dos seus websites e contactos telefónicos, um número tão alargado de incidentes.

55. E nem se pode argumentar que uma tal medida traria uma utilidade acrescida face ao que já é a prática do sector, quanto a isto. Com efeito, tanto a Cabovisão como os demais operadores, já prevêem diversas medidas de informação aos utilizadores de incidentes de segurança que afectem os serviços contratados pelo que uma obrigação adicional só irá implicar custos acrescidos, sem que seja devidamente fundamentada com a demonstração de um verdadeiro benefício ou contribuição para o reforço da segurança das redes e serviços de comunicações electrónicas.

56. Assim sendo, a abordagem preconizada pelo Regulador no Projecto de Decisão II é manifestamente desproporcional, não sendo de aceitar. O Regulador deve reanalisar a necessidade de adopção de um Projecto de Decisão desta natureza e, caso entenda ser de manter, deve limitar ao máximo os casos previstos como sendo 'divulgáveis' por interesse público, restringindo-os aos casos relativos a incidentes realmente graves, como sejam os incidentes que afectem o acesso ao número único de emergência 112 ou a entidades públicas relevantes (por exemplo, hospitais, forças de segurança e emergência).

57. Caso assim não se entenda, é de sublinhar que, em qualquer caso, nunca os critérios de divulgação ao público de incidentes devem replicar os patamares de notificação de incidentes de segurança ao ICP-ANACOM, previstos no Projecto de Decisão I.

58. Não faz sentido que se determine que é do interesse público que as empresas informem o público de um escopo tão alargado de incidentes de segurança pelo que, caso o Regulador conclua pela necessidade de adopção do Projecto de Decisão II, deverá rever os patamares que despoletam a obrigação de divulgação ao público, que têm necessariamente de ser menos exigentes.

**B. CONTEÚDOS, MEIOS E PRAZOS PARA A DIVULGAÇÃO**

59. Dado que os operadores já instituíram meios de disponibilização de informação ao público da ocorrência de incidentes de segurança, a Cabovisão não pode concordar com a imposição de uma obrigação de divulgação da informação na página electrónica do operador, em local de destaque, com a manutenção de um histórico de 6 meses de incidentes.

60. Esta intervenção é claramente excessiva e ultimamente inútil, podendo ser contraproducente face aos riscos de interpretações danosas ou ao aproveitamento malicioso por terceiros para exploração de potenciais vulnerabilidades das redes de comunicações electrónicas.

61. Caso o Regulador opte por manter o Projecto de Decisão em causa, deverá prever que é suficiente a divulgação ao público através de contacto telefónico (que abrange, necessariamente, o IVR).

62. Quanto à divulgação ao público no prazo de 1 hora, trata-se de um prazo insuficiente e irrealista do ponto de vista do tempo necessário à execução dos processos internos de gestão e comunicação de incidentes/crise e de canalização de esforços para a sua resolução. Também do ponto de vista dos utilizadores, tendo em conta a experiência da Cabovisão, a notificação no prazo de 1 hora revela-se desnecessariamente exigente.

63. O prazo não deverá nunca ser inferior ao prazo previsto para notificação à entidade reguladora – 2 dias.

**C. ENTRADA EM VIGOR E DISPOSIÇÃO TRANSITÓRIA**

64. O prazo estipulado para entrada em vigor destas alterações, de 30 dias, é manifestamente insuficiente e inviável.

65. Desde logo, a Cabovisão não concorda com a necessidade do presente Projecto de Decisão, devendo o ICP-ANACOM determinar, casuisticamente, quais os incidentes de segurança que revestem um interesse público que imponha a sua divulgação ao público em geral. Este era, indubitavelmente, o espírito do legislador quando adoptou a alínea b) do artigo 54.º-E

66. Mas caso o ICP-ANACOM assim não entenda, um prazo mínimo de 6 meses deve ser considerado.

Palmela, 27 de Janeiro de 2011

Madalena Sutcliffe

Direcção Jurídica e de Regulação