DECISÃO

Enquadramento

O ICP – Autoridade Nacional de Comunicações (ICP-ANACOM), por deliberação do Conselho de Administração de 22 de dezembro de 2011, aprovou 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; e
- 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.

Nos termos da mesma deliberação, foi 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 (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.

Concluídos os processos de audiência prévia e de consulta, foi elaborado o relatório correspondente, que se anexa à presente decisão e dela faz parte integrante, apresentando a síntese das respostas recebidas e o entendimento do ICP-ANACOM, fundamentando as opções tomadas nesta decisão.

Decisão

Assim, tendo presente as conclusões do relatório da audiência prévia e da consulta e ao abrigo do disposto na alínea d) do artigo 9.º dos Estatutos, anexos ao Decreto-Lei n.º 309/2001, de 7 de dezembro, no âmbito das atribuições previstas na alínea b) do artigo 6.º dos mesmos Estatutos e na alínea c) do n.º 1 e na alínea f) do n.º 4 do artigo 5.º da Lei das Comunicações Eletrónicas, e no exercício das competências previstas no n.º 2 do artigo 54.º-C e na alínea b) do artigo 54.º-E da mesma lei, o Conselho de Administração do ICP-ANACOM deliberou aprovar a decisão relativa:

- às circunstâncias, ao formato e aos 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 (ANEXO A); e

- à 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 (ANEXO B).

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 …… e do número de telefone ……; 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

b) 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

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[1], 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[2] 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.

---

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

[2] *Uniform Resource Locator*.

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.