Projeto de regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas

NOTA JUSTIFICATIVA

1. De entre as alterações introduzidas em 2009 à Diretiva-Quadro (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) pela Diretiva 2009/140/CE, do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, consta a introdução da regulamentação da matéria da segurança e integridade das redes e serviços, com o aditamento do Capítulo III-A.

2. Em transposição da Diretiva 2009/140/CE, a Lei n.º 51/2011, de 13 de setembro, veio, por seu turno, alterar a Lei das Comunicações Eletrónicas (Lei n.º 5/2004, de 10 de fevereiro, na sua redação em vigor), introduzindo a regulamentação da matéria da segurança e integridade das redes e serviços no novo Capítulo V do Título III, no qual são cometidas à ANACOM, entre outras, as seguintes competências específicas:

a) Aprovar medidas técnicas de execução e fixar requisitos adicionais a cumprir pelas empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público em matéria de segurança e integridade, para os efeitos do disposto no artigo 54.º-A e nos termos previstos no n.º 1 do artigo 54.º-C e no artigo 54.º-D da Lei das Comunicações Eletrónicas;

b) Aprovar 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 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, ao abrigo do disposto no artigo 54.º-B e no n.º 2 do artigo 54.º-C da Lei das Comunicações Eletrónicas;

c) Determinar as condições em que as empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público devem divulgar ao público as violações de segurança ou as perdas de integridade com impacte significativo no funcionamento das redes e serviços, ao abrigo do disposto na alínea *b)* do artigo 54.º-E da Lei das Comunicações Eletrónicas;

d) Determinar as obrigações de realização de auditorias à segurança das redes e serviços e de envio do respetivo relatório pelas empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público, bem como os requisitos a que devem obedecer as auditorias e as entidades auditoras, ao abrigo do disposto nos n.ºs 1 e 2 do artigo 54.º-F da Lei das Comunicações Eletrónicas.

3. Por decisão da ANACOM de 12 de dezembro de 2013, alterada por decisão de 8 de janeiro de 2014, a ANACOM concretizou as condições aplicáveis às obrigações de notificação e de divulgação ao público de violações de segurança ou perdas de integridade com impacte significativo no funcionamento das redes e serviços, tendo, a 12 de junho de 2014, entrado em funcionamento um centro de reporte, com funcionamento permanente, para a receção das notificações.

4. Tendo por base a experiência adquirida não só através da atividade do centro de reporte, mas também pela cooperação nacional e internacional nesta matéria, entende esta Autoridade ser este o momento oportuno para exercer as competências referidas no ponto 2, através da aprovação de um regulamento relativo à segurança e integridade das redes e serviços.

5. No que respeita, em particular, às obrigações de notificação e de divulgação ao público, entende esta Autoridade dever integrar neste regulamento o normativo que reflita as medidas já concretizadas ao abrigo da decisão de 12 de dezembro de 2013, cuja execução se entende ter vindo a decorrer de uma forma eficaz e consensual, sem prejuízo de algumas adaptações necessárias em face da experiência recolhida na atividade do centro de reporte. Por esta via e a bem da transparência e da segurança jurídica, congrega-se e consolida-se num único instrumento, um conjunto devidamente articulado de condições aplicáveis em matéria de segurança e integridade das redes e serviços.

6. Neste contexto e por decisão de 4 de agosto de 2016, a ANACOM aprovou o início do procedimento de elaboração de um regulamento relativo à segurança e integridade das redes e serviços, bem como a publicitação do respetivo anúncio nos termos previstos no n.º 1 do artigo 98.º do Código do Procedimento Administrativo.

Findo o prazo fixado, foram recebidos 18 contributos, os quais foram objeto de análise e ponderação na elaboração deste projeto.

7. Na regulamentação das obrigações das empresas em matéria de segurança e integridade das redes e serviços, foram objeto de ponderação, por um lado, os custos a incorrer pelas empresas no cumprimento das suas obrigações e, por outro, os benefícios daí emergentes, os quais incluem não só a defesa dos interesses dos cidadãos e, em particular, dos utilizadores das redes e serviços, o suporte à continuidade da prestação de serviços relevantes à sociedade e aos cidadãos, a garantia do acesso aos serviços de emergência e, em geral, a promoção do desenvolvimento do mercado interno por via da melhoria da fiabilidade das redes e serviços, como também aqueles resultantes da prevenção de incidentes de segurança e do impedimento ou minimização do respetivo impacte.

8. Assim, ao abrigo do disposto na alínea *m)* do n.º 1 do artigo 8.º, na alínea *a)* do n.º 2 do artigo 9.º, no artigo 10.º e na alínea *b)* do n.º 1 do artigo 26.º dos Estatutos da ANACOM, aprovados pelo Decreto-Lei n.º 39/2015, de 16 de março, e nos termos previstos na alínea *c)* do n.º 1 e na alínea *f)* do n.º 4, ambos do artigo 5.º, dos artigos 54.º-A, 54.º-B, 54.º-C, 54.º-D, da alínea *b)* do artigo 54.º-E e dos n.os 1 e 2 do artigo 54.º-F da Lei das Comunicações Eletrónicas, a ANACOM aprovou, por decisão de 29 de dezembro de 2016, o presente projeto de regulamento relativo à segurança e integridade das redes e serviços, que, nos termos do disposto no artigo 10.º dos seus Estatutos e dos artigos 98.º e seguintes do Código do Procedimento Administrativo e para os efeitos previstos no artigo 8.º e, em especial, no n.º 4 do artigo 54.º-C da Lei das Comunicações Eletrónicas, se submete ao devido procedimento de consulta pública, a decorrer pelo período de 30 dias úteis, mediante publicação no sítio institucional da ANACOM na *Internet* e na 2.ª Série do Diário da República.

9. Neste contexto, solicita-se aos interessados que enviem os respetivos contributos, por escrito e em língua portuguesa, preferencialmente por correio eletrónico para o endereço regulamento.seguranca@anacom.pt.

Encerrada a consulta pública, a ANACOM procederá à apreciação dos contributos apresentados pelos interessados e, com a aprovação deste regulamento, disponibilizará um relatório contendo referência a todos os contributos recebidos, bem como uma apreciação global que reflita o entendimento desta Autoridade sobre os mesmos e os fundamentos das opções tomadas.

Projeto de regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas

TÍTULO I

Disposições gerais

Artigo 1.º

Objeto

O presente regulamento estabelece:

a) As medidas técnicas de execução e os requisitos adicionais a cumprir pelas empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público em matéria de segurança e integridade, para os efeitos do disposto no artigo 54.º-A e nos termos previstos no n.º 1 do artigo 54.º-C e no artigo 54.º-D da Lei das Comunicações Eletrónicas e nos termos previstos no Título II;

b) As circunstâncias, o formato e os procedimentos aplicáveis às exigências de comunicação de violações de segurança ou perdas de integridade das redes 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, ao abrigo do disposto no artigo 54.º-B e no n.º 2 do artigo 54.º-C da Lei das Comunicações Eletrónicas e nos termos previstos no Capítulo I do Título III;

c) As condições em que as empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público devem divulgar ao público as violações de segurança ou as perdas de integridade com impacte significativo no funcionamento das redes e serviços, ao abrigo do disposto na alínea *b)* do artigo 54.º-E da Lei das Comunicações Eletrónicas e nos termos previstos no Capítulo II do Título III;

d) As obrigações de realização de auditorias à segurança das redes e serviços e de envio do respetivo relatório pelas empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público, bem como os requisitos a que devem obedecer as auditorias e as

entidades auditoras, ao abrigo do disposto nos n.os 1 e 2 do artigo 54.º-F da Lei das Comunicações Eletrónicas e nos termos previstos no Título IV.

Artigo 2.º

Âmbito

1 – As empresas devem assegurar que o cumprimento das suas obrigações em matéria de segurança e integridade das redes e serviços previstas na lei e no presente regulamento abrange:

a) As condições normais de funcionamento;

b) As situações extraordinárias, incluindo, entre outras, as seguintes situações:

i) Violação de segurança ou perda de integridade com impacte significativo;

ii) Rutura da rede, emergência ou força maior, nos termos previstos no n.º 1 do artigo 49.º da Lei das Comunicações Eletrónicas;

iii) Exceções previstas nas alíneas *a)*, *b)* e *c)* do n.º 3 do artigo 3.º do Regulamento (UE) n.º 2015/2120 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015, que estabelece medidas respeitantes ao acesso à *Internet* aberta;

iv) Acidente grave ou catástrofe, bem como as situações de alerta, contingência e calamidade, nos termos previstos nas disposições legais e regulamentares aplicáveis em matéria de proteção civil;

v) Estado de emergência, estado de sítio ou estado de guerra, nos termos previstos nas disposições legais e regulamentares aplicáveis em matéria de planeamento civil de emergência;

vi) Ativação de plano de emergência de proteção civil ou de planeamento civil de emergência, nos termos previstos nas disposições legais e regulamentares aplicáveis;

vii) Grave ameaça à segurança interna, incluindo as situações de ataques terroristas ou de acidentes graves ou catástrofes, nos termos previstos nas disposições legais e regulamentares aplicáveis em matéria de segurança interna.

2 – As empresas devem cumprir as suas obrigações em matéria de segurança e integridade das redes e serviços, previstas na lei e no presente regulamento, de um modo adequado a permitir o cumprimento das suas demais obrigações no âmbito da oferta de redes e serviços de comunicações eletrónicas, incluindo:

a) As obrigações em matéria de disponibilidade dos serviços e de acesso aos serviços de emergência, nos termos previstos nas disposições legais e regulamentares aplicáveis;

b) As obrigações no âmbito do planeamento civil de emergência, dos planos de emergência de proteção civil e da segurança interna, nos termos previstos nas disposições legais e regulamentares aplicáveis;

c) Quando aplicáveis, as obrigações emergentes dos contratos para a prestação do serviço universal.

3 – As empresas devem assegurar que o cumprimento das suas obrigações em matéria de segurança e integridade das redes e serviços previstas na lei e no presente regulamento abrange todos os ativos, de sua propriedade ou gestão, incluindo os equipamentos localizados nas instalações dos clientes, necessários para a utilização das suas redes ou dos seus serviços.

Artigo 3.º

Definições

1 – Para os efeitos do disposto no presente regulamento, entende-se por:

a) «*Ameaça*», causa potencial de um incidente de segurança;

b) «*Análise dos Riscos*», o procedimento de análise dos riscos para a segurança e integridade das redes e serviços a realizar pelas empresas nos termos previstos no Artigo 9.º;

c) «*Ativos*», as infraestruturas, os sistemas de transmissão ou de informação, os equipamentos e os demais recursos, físicos e lógicos, que compõem ou suportam uma rede de comunicações públicas e respetivos acessos, incluindo interligações, um serviço de comunicações eletrónicas acessível ao público ou um serviço conexo associado;

d) «*Auditora*», a entidade auditora responsável pela realização de auditoria à segurança das redes e serviços ao abrigo do disposto nos n.ºs 1 e 2 do artigo 54.º-F da Lei das Comunicações Eletrónicas e nos termos previstos no Artigo 31.º;

e) «*Auditoria*», a auditoria à segurança das redes e serviços a realizar pelas empresas, ao abrigo do disposto nos n.os 1 e 2 do artigo 54.º-F da Lei das Comunicações Eletrónicas e nos termos previstos no Título IV;

f) «*Empresas*», as empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público, nos termos definidos na Lei das Comunicações Eletrónicas;

g) «*Incidente de segurança*», evento com impacte negativo real no funcionamento ou na segurança ou integridade das redes e serviços, incluindo violação de segurança ou perda de integridade com impacte no funcionamento das redes e serviços;

h) «*Lei das Comunicações Eletrónicas*», a Lei n.º 5/2004, de 10 de fevereiro, na sua redação em vigor;

i) «*Responsável pela Segurança*», o colaborador da empresa, responsável pela gestão da segurança e integridade das redes e serviços e pela sua representação no exercício das funções que lhe são cometidas pelo presente regulamento, nos termos previstos no Artigo 20.º;

j) «*Risco*», efeito de evento, ou de sequência de eventos, reais ou potenciais e razoavelmente identificáveis, que consiste num impacte negativo potencial no funcionamento ou na segurança ou integridade das redes e serviços;

k) «*Segurança das redes e serviços*», a capacidade das redes ou dos serviços de comunicações eletrónicas, incluindo os serviços conexos associados, para resistir, com um dado nível de confiança, a qualquer ameaça ou risco que comprometa a disponibilidade, a autenticidade, a integridade ou a confidencialidade dos dados armazenados, transmitidos ou tratados ou dos serviços relacionados oferecidos ou acessíveis através dessas redes ou serviços;

l) «*Violação de segurança ou perda de integridade com impacte significativo*», a violação de segurança ou perda de integridade com o impacte previsto nos termos do Artigo 24.º;

m) «*Vulnerabilidade*», caraterística de um ativo ou de uma medida que pode ser explorada por uma ou mais ameaças.

2 – Para efeitos do disposto no presente regulamento, todas as referências ao território da Região Autónoma da Madeira consideram-se preenchidas quando a área geográfica em causa abranja o território das ilhas da Madeira e do Porto Santo.

Artigo 4.º

Cooperação e partilha de informação

1 – As empresas devem cooperar com a ANACOM no âmbito da prossecução das suas atribuições e do exercício das suas competências nas matérias de segurança e integridade das redes e serviços.

2 – As empresas devem cooperar entre si no cumprimento das suas obrigações em matéria de segurança e integridade das redes e serviços, incluindo, em especial, nas seguintes situações:

a) Riscos, ameaças ou vulnerabilidades, comuns ou de efeito em cascata;

b) Dependência ou interdependência entre as redes ou serviços, incluindo, entre outros casos, o acesso e a interligação de redes, a co-localização de ativos e a partilha de infraestruturas ou de outros recursos;

c) Fornecimentos comuns de bens ou serviços por terceiros.

3 – Para efeitos do disposto no número anterior, as empresas devem cooperar, consoante adequado, através da realização de ações conjuntas, da celebração de acordos de assistência mútua, da troca de pontos de contacto permanentes ou da partilha de informação.

TÍTULO II

Obrigações das empresas em matéria de segurança e integridade

CAPÍTULO I

Disposições gerais

Artigo 5.º

Obrigações das empresas

1 – Ao abrigo do disposto no artigo 54.º-A da Lei das Comunicações Eletrónicas e nos termos previstos no presente regulamento:

a) As empresas devem adotar as medidas técnicas e organizacionais adequadas à prevenção, gestão e redução dos riscos para a segurança das redes e serviços visando, em especial, impedir ou minimizar o impacte

dos incidentes de segurança nas redes interligadas, a nível nacional e internacional, e nos utilizadores;

b) As empresas que oferecem redes de comunicações públicas devem adotar as medidas adequadas para garantir a integridade das respetivas redes, assegurando a continuidade da prestação dos serviços que nelas se suportam.

2 – As empresas devem assegurar que os procedimentos e as medidas técnicas e organizacionais adotadas para cumprimento do disposto na lei e no presente regulamento:

a) São conformes com as decisões da Comissão Europeia adotadas ao abrigo do procedimento previsto no artigo 13.º-A da Diretiva n.º 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, na sua redação em vigor;

b) São baseadas, na ausência das decisões previstas na alínea anterior, nas normas, especificações e recomendações europeias e internacionais existentes sobre a matéria;

c) Têm em consideração os documentos técnicos publicados pela Agência Europeia para a Segurança das Redes e da Informação (ENISA) em resultado dos trabalhos desenvolvidos ao nível da aplicação da Diretiva n.º 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, na sua redação em vigor.

3 – Para efeitos do disposto das alíneas *b)* e *c)* do número anterior, a ANACOM publica, no seu sítio institucional na *Internet*:

a) Uma lista das normas, especificações e recomendações europeias e internacionais existentes sobre a matéria;

b) Uma lista dos documentos técnicos publicados pela Agência Europeia para a Segurança das Redes e da Informação (ENISA).

Artigo 6.º

Medidas técnicas de execução e requisitos adicionais

1 – Sem prejuízo do disposto no Artigo 5.º e para efeitos do disposto no n.º 1 do artigo 54.º-C e do artigo 54.º-D da Lei das Comunicações Eletrónicas, as

empresas devem adotar as seguintes medidas técnicas de execução e requisitos adicionais:

a) Classificar os ativos e elaborar o Inventário de Ativos, nos termos previstos, respetivamente, nos Artigo 7.º e Artigo 8.º;

b) Assegurar a realização de Análises dos Riscos e adotar as medidas técnicas e organizacionais adequadas, nos termos previstos no Artigo 9.º, as quais incluem, em qualquer caso e pelo menos, as seguintes medidas e requisitos:

i) Medidas de redundância, de robustez e de resiliência, nos termos previstos no Artigo 10.º;

ii) Procedimentos de controlo da gestão excecional de tráfego de acesso à *Internet*, nos termos previstos no Artigo 11.º;

iii) Procedimentos de gestão de alterações, nos termos previstos no Artigo 12.º;

iv) Um sistema de controlo de acessos, nos termos previstos no Artigo 13.º;

v) Um sistema de monitorização e controlo, nos termos previstos no Artigo 14.º;

vi) Elaboração e execução de um programa anual de exercícios, nos termos previstos no Artigo 15.º;

c) Prestar informações aos seus clientes, nos termos previstos no Artigo 16.º;

d) Elaborar e enviar à ANACOM:

i) Uma Caracterização Geral da Segurança, nos termos previstos no Artigo 17.º;

ii) Um Plano de Segurança, nos termos previstos no Artigo 18.º;

iii) Um Relatório Anual de Segurança, nos termos previstos no Artigo 19.º;

e) Dotar-se da estrutura e dos recursos adequados ao cumprimento das suas obrigações em matéria de segurança e integridade das redes e serviços, incluindo:

i) A designação de um Responsável pela Segurança, nos termos previstos no Artigo 20.º;

ii) A designação de um Ponto de Contacto Permanente, nos termos previstos no Artigo 21.º;

iii) O acesso a equipa de resposta a incidentes de segurança, nos termos previstos no Artigo 22.º;

f) Compilar e atualizar o *Dossier* de Segurança, nos termos previstos no Artigo 23.º.

2 – Para efeitos do disposto na alínea *b)* do número anterior, as medidas a adotar ao abrigo do disposto nos artigos 10.º a 15.º devem ser reforçadas pelas empresas sempre que necessário e na medida adequada em resposta aos resultados das Análises de Risco realizadas.

3 – Para efeitos do disposto na alínea *e)* do n.º 1, as empresas devem estabelecer e manter uma estrutura apropriada de funções e responsabilidades de segurança, bem como assegurar que estão dotadas da capacidade técnica necessária, nomeadamente ao nível dos recursos humanos, dos ativos e dos fornecimentos por terceiros, para garantir o cumprimento das suas obrigações em matéria de segurança e integridade das redes e serviços, nos termos previstos na lei e no presente regulamento.

CAPÍTULO II

Medidas técnicas de execução e requisitos adicionais

Artigo 7.º

Classificação de ativos

1 – As empresas devem classificar os seus ativos numa classe de A a D, nos termos previstos no presente artigo.

2 – Um ativo deve ser classificado na classe A se, em resultado de interrupção ou perturbação grave do seu funcionamento, o número de assinantes ou de acessos afetados possa ser igual ou superior a 500.000 ou a área geográfica afetada possa ser igual ou superior a 3.000 Km2 ou abranger a totalidade do território da Região Autónoma dos Açores ou da Região Autónoma da Madeira.

3 – Devem ainda ser classificados na classe A os seguintes ativos:

a) O centro principal de gestão e operação de uma empresa que, no conjunto das suas ofertas, tenha um número total de assinantes ou de acessos igual ou superior a 500.000;

b) O centro principal de gestão e operação de uma empresa que inclua, pelo menos, um ativo da classe A;

c) Os ativos de que dependa a oferta de redes e serviços através dos quais seja assegurada a continuidade da prestação dos serviços previstos na alínea *f)* do n.º 3 do Artigo 24.º;

d) Os ativos que assegurem interligação internacional, interligação entre as Regiões Autónomas ou interligação entre o Continente e uma Região Autónoma, incluindo estação de cabos submarinos, estação de satélites ou sistema terrestre transfronteiriço;

e) Os ativos que assegurem interligação entre redes que, no seu conjunto, suportem ofertas dirigidas a um número total de assinantes ou de acessos igual ou superior a 500.000.

4 – Um ativo deve ser classificado na classe B se, em resultado de interrupção ou perturbação grave do seu funcionamento, o número de assinantes ou de acessos afetados possa ser inferior a 500.000 e igual ou superior a 100.000 ou a área geográfica afetada possa ser inferior a 3.000 km2 e igual ou superior a 2.000 Km2 ou abranger a totalidade do território de uma ilha da Região Autónoma dos Açores ou da Região Autónoma da Madeira, exceto quando, nos termos previstos nos números anteriores, deva ser classificado na classe A.

5 – Devem ainda ser classificados na classe B os seguintes ativos, quando não devam ser classificados na classe A:

a) O centro principal de gestão e operação de empresa que, no conjunto das suas ofertas, tenha um número de assinantes ou de acessos inferior a 500.000 e igual ou superior a 100.000;

b) O centro principal de gestão e operação que inclua, pelo menos, um ativo classificado na classe B;

c) Os ativos que assegurem interligação inter-ilhas nas Regiões Autónomas dos Açores ou da Madeira, incluindo estação de cabos submarinos e estação de satélites;

d) Os ativos que assegurem interligação entre redes que, no seu conjunto, suportem ofertas dirigidas a um número total de assinantes ou de acessos inferior a 500.000 e igual ou superior a 100.000.

6 – Um ativo deve ser classificado na classe C se, em resultado de interrupção ou perturbação grave do seu funcionamento, o número de assinantes ou de acessos afetados possa ser inferior a 100.000 e igual ou superior a 10.000 ou a área geográfica afetada possa ser inferior a 2.000 Km2 e superior ou igual a

1.000 Km2, exceto quando, nos termos previstos nos números anteriores, deva ser classificado na classe A ou na classe B.

7 – Um ativo deve ser classificado na classe D sempre que não deva ser classificado em nenhuma das classes A, B ou C.

8 – As empresas devem ainda classificar os ativos identificados no âmbito do planeamento civil de emergência ou de um plano de emergência de proteção civil que a ANACOM indique através de notificação às mesmas, a qual inclui:

a) A identificação do ativo;

b) A classe na qual o ativo deve ser classificado.

Artigo 8.º

Inventário de Ativos

1 – As empresas devem elaborar e manter atualizado um Inventário de Ativos, assinado pelo Responsável pela Segurança, que inclua:

a) Os ativos classificados nas classes A, B ou C;

b) Os ativos críticos para a continuidade do funcionamento das suas redes ou serviços.

2 – Para cada elemento do Inventário de Ativos deve constar a seguinte informação:

a) Identificador único;

b) Designação;

c) Caraterização em termos de:

i) Funcionalidades e serviços suportados;

ii) Indicação da classe na qual foi classificado, ao abrigo do disposto no Artigo 7.º, e descrição do impacte potencial de uma interrupção ou de uma perturbação grave do seu funcionamento;

iii) Medidas, controlos e registos de segurança adotados;

iv) Fornecimentos de terceiros críticos para o seu funcionamento, incluindo serviços de gestão, de operação, de segurança e de energia;

v) Autonomia em caso de falha de fornecimento de energia;

vi) Localização geográfica e identificação das entidades detentoras ou gestoras dos locais;

vii) No caso de interligação, indicação do tipo (interligação internacional, interligação entre as Regiões Autónomas, interligação entre o Continente e as Regiões Autónomas ou interligação inter-ilhas) e identificação das empresas interligadas;

d) Registo de incidentes de segurança ocorridos;

e) Registo das alterações efetuadas, incluindo os resultados dos testes de integração e de sistema realizados e os planos de restauro dos ativos, nos termos previstos no Artigo 12.º;

f) Referência à Análise dos Riscos mais recente.

3 – As empresas devem elaborar o Inventário de Ativos no prazo de 60 dias úteis a contar da data de início de atividade.

4 – As empresas devem comunicar à ANACOM uma síntese do Inventário de Ativos que contenha uma lista de elementos que inclua a informação constante das alíneas *a)* e *b)* e das subalíneas *ii)* e *vi)* da alínea *c)* do n.º 2:

a) Na sua versão inicial, no prazo previsto no número anterior;

b) Numa versão atualizada, em conjunto com o Relatório Anual de Segurança.

Artigo 9.º

Gestão dos riscos

1 – As empresas devem realizar uma Análise dos Riscos:

a) De âmbito global, em relação aos ativos classificados ou classificáveis nas classes A, B ou C ou críticos para a continuidade do funcionamento das suas redes ou serviços:

i) Pelo menos, uma vez por ano;

ii) Após a notificação, por parte da ANACOM, de um risco, de uma ameaça ou de uma vulnerabilidade emergentes que impliquem uma elevada probabilidade de ocorrência de violação de segurança ou perda de integridade com impacte significativo, dentro do prazo que a ANACOM, caso assim o entenda, fixe para o efeito;

b) De âmbito parcial:

i) Após cada notificação da identificação de cliente ao abrigo do disposto no n.º 6 do Artigo 24.º, em relação aos ativos de que dependa a oferta de redes e serviços através dos quais seja assegurada a continuidade da prestação dos respetivos serviços relevantes;

ii) Após cada notificação da identificação de ativo ao abrigo do disposto no n.º 8 do Artigo 7.º, em relação aos mesmos;

iii) Durante o planeamento e preparação da introdução de uma alteração a ativo ou ativos integrados no Inventário de Ativos, em relação ao ativo ou ativos envolvidos;

iv) Após a ocorrência de uma violação de segurança ou perda de integridade com impacte significativo ou outra situação extraordinária, em relação aos ativos afetados integrados no Inventário de Ativos.

2 – As empresas devem documentar a preparação, a execução e a apresentação dos resultados da Análise dos Riscos.

3 – As empresas devem garantir que a Análise dos Riscos abranja, para cada ativo:

a) A identificação das ameaças, internas ou externas, intencionais ou não intencionais, incluindo:

i) De acidentes ou desastres naturais;

ii) De erros humanos;

iii) De ataques maliciosos;

iv) De falhas de *hardware* ou de *software*;

v) De falhas no fornecimento de bens ou serviços por entidade externa;

b) A caracterização do impacte e da probabilidade da ocorrência das ameaças identificadas na alínea anterior.

4 – A Análise dos Riscos deve ter em consideração:

a) O histórico de situações extraordinárias ocorridas;

b) O histórico de incidentes de segurança e, em especial, de violações de segurança ou perdas de integridade com impacte significativo;

c) O número de assinantes ou de acessos envolvidos;

d) A área geográfica envolvida;

e) A garantia de acesso aos serviços de emergência;

f) O suporte à continuidade da prestação dos serviços previstos na alínea *f)* do n.º 3 do Artigo 24.º.

5 – A Análise dos Riscos deve ainda ter em consideração a avaliação integrada dos riscos para a segurança e integridade das redes e serviços, a nível nacional, europeu e internacional, publicada anualmente ou notificada às empresas pela ANACOM.

6 – Na sequência de cada Análise dos Riscos, as empresas devem:

a) Rever a classificação dos ativos e, se necessário, proceder à sua reclassificação e à atualização do Inventário de Ativos;

b) Adotar as medidas técnicas e organizacionais adequadas, incluindo, entre outras, as medidas e os requisitos previstos nos artigos 10.º a 15.º;

c) Rever e, se necessário, atualizar a Caraterização Geral de Segurança, o Plano de Segurança e a demais documentação integrada no *Dossier* de Segurança.

7 – As medidas a adotar ao abrigo do disposto no número anterior devem permitir:

a) A prevenção, a gestão e a redução dos riscos;

b) O reforço da robustez e da resiliência dos ativos, incluindo:

i) A sua proteção contra as ameaças identificadas;

ii) A sua recuperação ou redundância, de forma a um rápido restauro do funcionamento das suas redes e serviços;

c) Uma resposta eficaz a incidentes de segurança, a ameaças ou a vulnerabilidades;

d) O acesso aos serviços de emergência;

e) O suporte à continuidade da prestação dos serviços previstos na alínea *f)* do n.º 3 do Artigo 24.º.

8 – Para efeitos do disposto no presente artigo, a ANACOM pode, caso assim o entenda necessário, emitir orientações com vista a uma harmonização da matriz de risco a adotar pelas empresas.

Artigo 10.º

Medidas de Redundância, de Robustez e de Resiliência

1 – As empresas devem, em relação aos ativos classificados na classe A:

a) Assegurar a sua redundância mediante o estabelecimento de ativos alternativos em local geográfico distinto;

b) Identificar o prazo necessário e caracterizar o procedimento para a ativação dos ativos alternativos referidos na alínea anterior.

2 – Em caso de impossibilidade de redundância dos ativos classificados na classe A, as empresas devem adotar medidas alternativas e comunicar à ANACOM a sua adoção e o respetivo fundamento, incluindo os resultados dos testes realizados.

3 – Excetua-se do disposto nos números anteriores os ativos classificados na classe A ao abrigo da alínea *c)* do n.º 3 do Artigo 7.º, em relação aos quais as empresas devem apenas dispor da capacidade de assegurar a redundância caso a mesma seja solicitada pelo cliente.

4 – As empresas devem assegurar a redundância das ligações entre os ativos classificados nas classes A, B ou C e, no caso das ligações entre os ativos classificados nas classes A ou B, que tais ligações sigam percursos geográficos distintos.

5 – As empresas devem identificar e caracterizar as medidas de robustez e de resiliência adotadas para os ativos classificados nas classes A, B ou C em resultado das Análises dos Riscos realizadas e tendo em consideração as ameaças com maior probabilidade de ocorrência ou com maior impacte potencial e, em qualquer caso:

a) De interrupções de fornecimento de energia;

b) De interrupções de fornecimento de circuito alugado;

c) De falhas de *hardware* ou de *software*;

d) De ataque malicioso;

e) De outras ameaças que a experiência e as boas práticas recolhidas a nível nacional e internacional justifique acautelar.

6 – As empresas devem assegurar que os ativos classificados nas classes A, B ou C estão dotados de sistema de alimentação de energia de emergência que lhes permita assegurar o seu funcionamento sem perturbação ou interrupção em caso de interrupção de fornecimento de energia com a seguinte duração mínima:

a) 24 horas para os ativos classificados na classe A;

b) 12 horas para os ativos classificados na classe B,

c) Seis horas para os ativos classificados na classe C.

7 – As empresas devem realizar testes às medidas a que se refere o presente artigo, incluindo testes ao funcionamento dos sistemas de alimentação de energia de emergência, com uma periodicidade mínima semestral, elaborando o registo da sua realização e dos resultados obtidos.

Artigo 11.º

Procedimentos de Controlo da Gestão Excecional de Tráfego no Acesso à *Internet*

1 – As empresas devem assegurar que a adoção de medidas de gestão de tráfego no acesso à *Internet* é feita em conformidade com o disposto no Regulamento (UE) n.º 2015/2120 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015, que estabelece medidas respeitantes ao acesso à *Internet* aberta.

2 – As empresas devem assegurar o registo da informação relevante para o controlo das medidas de gestão excecional de tráfego no acesso à *Internet*, que, em relação a cada medida adotada, inclua, entre outros, os seguintes elementos:

a) A exceção que a fundamenta, nos termos previstos nas alíneas *a)*, *b) ou c)* do n.º 3 do artigo 3.º do Regulamento (UE) n.º 2015/2120 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015, devidamente documentada;

b) A natureza da medida, nomeadamente de bloqueio, de abrandamento, de alteração, de restrição, de degradação ou outra;

c) O objeto da medida, nomeadamente os conteúdos, as aplicações ou os serviços e os portos ou endereços IP abrangidos;

d) A duração, incluindo as datas e horas de início e de termo da medida.

3 – As empresas devem adotar, identificar e caraterizar um Sistema para a Monitorização do Tráfego no Acesso à *Internet*, de modo contínuo, para a deteção:

a) De ameaças ao funcionamento ou à segurança e integridade da rede, dos serviços prestados através dela e dos equipamentos terminais dos utilizadores finais;

b) De congestionamentos iminentes da rede.

4 – No respeitante à prevenção e atenuação de situações de congestionamento da rede, as empresas devem garantir que as medidas de gestão excecional do tráfego no acesso à *Internet* adotadas permitam ainda assegurar a adoção das medidas necessárias:

a) À reserva de capacidade para comunicações de emergência de interesse público;

b) À priorização de tráfego nas situações extraordinárias previstas nas subalíneas *iv)* a *vii)* da alínea *b)* do n.º 1 do Artigo 2.º.

Artigo 12.º

Procedimentos de Gestão de Alterações

1 – As empresas devem estabelecer Procedimentos de Gestão de Alterações a fim de minimizar a probabilidade de ocorrência de incidente de segurança que possa resultar dessas alterações.

2 – Em especial no caso de alterações físicas ou lógicas aos ativos classificados nas classes A ou B, as empresas devem:

a) Assegurar a realização de testes de integração e de sistema antes da introdução da alteração;

b) Elaborar plano de restauro dos ativos adequado à alteração a introduzir.

Artigo 13.º

Sistemas de Controlo de Acessos

1 – As empresas devem estabelecer e manter Sistemas de Controlo de Acessos físicos e lógicos que tenha em especial consideração os ativos constantes do Inventário de Ativos.

2 – Os Sistemas de Controlo de Acessos devem:

a) Ser adequados à prevenção, à gestão e à redução dos riscos para a segurança e integridade das redes e serviços;

b) Ser revistos com uma periodicidade mínima anual e sempre que necessário, nomeadamente em resultado das Análises dos Riscos realizadas.

3 – As empresas devem realizar testes aos Sistemas de Controlo de Acessos, com uma periodicidade mínima semestral, com vista à proteção contra acessos não autorizados.

4 – As empresas devem assegurar a documentação e o registo da operação dos Sistemas de Controlo de Acessos, que inclua:

a) As alterações introduzidas;

b) Os incidentes de segurança ocorridos;

c) Os testes realizados;

d) Os alarmes gerados.

Artigo 14.º

Sistemas de Monitorização e Controlo

1 – As empresas devem estabelecer e manter Sistemas de Monitorização e Controlo das condições de funcionamento, da segurança e integridade dos ativos constantes do Inventário de Ativos e do tráfego, que operem em modo contínuo e que permitam:

a) A deteção de ameaças e de incidentes de segurança;

b) A geração dos alarmes adequados no caso da sua ocorrência;

c) A ativação de medidas de segurança.

2 – Os Sistemas de Monitorização e Controlo devem:

a) Ser adequados à prevenção, à gestão e à redução dos riscos para o funcionamento e para a segurança e integridade das redes e serviços;

b) Ser revistos com uma periodicidade mínima anual e sempre que necessário, nomeadamente em resultado das Análises dos Riscos realizadas.

3 – As empresas devem realizar testes aos Sistemas de Monitorização e Controlo, com uma periodicidade mínima semestral.

4 – As empresas devem assegurar a documentação e o registo da operação dos Sistemas de Monitorização e Controlo, que inclua:

a) As ameaças detetadas;

b) Os incidentes de segurança ocorridos;

c) Os alarmes gerados;

d) As medidas ativadas;

e) Os testes realizados;

f) As alterações introduzidas.

Artigo 15.º

Exercícios

1 – As empresas devem elaborar um Programa Anual de Exercícios de avaliação da segurança e integridade com vista à melhoria das medidas técnicas e organizacionais adotadas, em especial no que respeita, quando aplicável:

a) Aos ativos constantes do Inventário de Ativos;

b) Ao acesso aos serviços de emergência;

c) Ao acesso às ofertas de redes e serviços;

d) Ao suporte à continuidade da prestação dos serviços previstos na alínea *f)* do n.º 3 do Artigo 24.º.

2 – O Programa Anual de Exercícios deve incluir as seguintes fases:

a) Fase de preparação;

b) Fase de realização;

c) Fase de avaliação.

3 – As empresas devem ainda assegurar que a execução do Programa Anual de Exercícios permita avaliar e testar o Plano de Segurança e, em especial, os respetivos planos de continuidade ou de restauro, verificando:

a) A sua eficácia na resposta aos riscos, às vulnerabilidades ou às ameaças, internas ou externas, intencionais ou não intencionais, com maior probabilidade de ocorrência ou com maior impacte potencial;

b) A conformidade com o disposto nas normas legais e regulamentares aplicáveis.

4 – As empresas devem assegurar, na medida do adequado, a participação de outras empresas ou de terceiros na execução do Programa Anual de Exercícios, designadamente mediante a realização de exercícios conjuntos.

5 – As empresas devem elaborar relatórios da execução do Programa Anual de Exercícios, incluindo a descrição dos resultados obtidos.

Artigo 16.º

Prestação de informação aos clientes

As empresas devem comunicar aos seus clientes previstos no n.º 6 do Artigo 24.º, com conhecimento da ANACOM, as medidas adotadas na sequência de incidentes de segurança ou em reação a ameaças ou a vulnerabilidades.

Artigo 17.º

Caracterização Geral da Segurança

1 – As empresas devem elaborar e manter atualizada uma Caraterização Geral da Segurança, que contenha os seguintes elementos:

a) A informação sobre a abordagem e a metodologia de segurança e de gestão dos riscos adotadas;

b) A política de segurança;

c) A descrição do sistema de gestão de segurança;

d) A descrição das medidas de redundância, de robustez e de resiliência;

e) A descrição do Sistema para a Monitorização do Tráfego de Acesso à *Internet*;

f) A descrição dos Sistemas de Controlo de Acessos;

g) A descrição dos Sistemas de Monitorização e Controlo;

h) A identificação e os contactos do Responsável pela Segurança, incluindo:

i) O nome;

ii) Endereço de correio eletrónico;

iii) Endereço geográfico;

i) Os contactos do Ponto de Contacto Permanente e, quando aplicável, do Ponto de Contacto Alternativo, incluindo:

i) A designação da função;

ii) Número de telefone fixo principal;

iii) Número de telefone móvel principal;

iv) Endereço de correio eletrónico;

v) Contactos alternativos;

vi) Endereço geográfico do local onde é assegurada a função.

2 – A informação prevista na alínea *h)* do número anterior deve ser instruída com uma declaração expressa, assinada por quem vincule a empresa, de que o Responsável pela Segurança se encontra devidamente mandatado, nos termos legalmente previstos, para representar a empresa no exercício das funções cometidas pelo presente regulamento.

3 – As empresas devem enviar à ANACOM, no prazo de cinco dias úteis a contar do início da sua atividade, a Caraterização Geral da Segurança, assinada pelo Responsável pela Segurança, bem como comunicar, com a antecedência mínima de 10 dias úteis em relação à sua adoção, de qualquer alteração à mesma.

Artigo 18.º

Plano de Segurança

1 – As empresas devem elaborar um Plano de Segurança que contemple todas as medidas técnicas e organizacionais adotadas.

2 – O Plano de Segurança deve ter como objetivos gerais:

a) Proteger a segurança e a integridade, físicas e lógicas, das redes e serviços;

b) Recuperar rapidamente o funcionamento das redes e serviços em caso de ocorrência de incidente de segurança;

c) Melhorar o nível de segurança e integridade das redes e serviços;

d) Assegurar a coordenação das ações entre a empresa e as demais entidades envolvidas, incluindo a ANACOM, as demais autoridades competentes, as outras empresas e, se aplicável, os clientes previstos no n.º 6 do Artigo 24.º.

3 – Em especial, o Plano de Segurança deve também incluir:

a) Planos de continuidade ou de restauro específicos para os ativos constantes do Inventário de Ativos;

b) As medidas necessárias para a salvaguarda de reserva de capacidade para comunicações de emergência de interesse público;

c) As medidas necessárias em matéria de congestionamento de redes em situações de emergência, incluindo os procedimentos a cumprir pela empresa.

4 – As empresas devem manter o Plano de Segurança atualizado e revisto com uma periodicidade mínima anual e sempre que necessário, em resultado das Análises dos Riscos realizadas.

Artigo 19.º

Relatório Anual de Segurança

1 – As empresas devem elaborar um Relatório Anual de Segurança com especial enfoque nos ativos constantes do Inventário de Ativos, que, de forma completa, mas sucinta, contenha os seguintes elementos:

a) Descrição das atividades desenvolvidas em matéria de segurança e integridade das redes e serviços e dos resultados atingidos, nomeadamente:

i) Análises dos Riscos;

ii) Exercícios;

iii) Auditorias;

b) Análise agregada dos incidentes de segurança com maior impacte e de todas as violações de segurança ou perdas de integridade com impacte significativo;

c) Síntese das principais alterações ao Plano de Segurança e das melhorias introduzidas nas medidas técnicas e organizacionais adotadas;

d) Recomendações de atividades, medidas ou práticas de cooperação entre empresas e a ANACOM que promovam a melhoria da segurança e integridade, agregadas, das redes e serviços;

e) Qualquer outra informação relevante.

2 – O Relatório Anual de Segurança deve ainda incluir o Programa Anual de Exercícios do ano seguinte ao qual aquele se reporta.

3 – As empresas devem apresentar o Relatório Anual de Segurança à ANACOM, assinado pelo Responsável pela Segurança, até ao último dia útil do mês de janeiro do ano seguinte ao qual o mesmo se reporta.

Artigo 20.º

Responsável pela Segurança

1 – As empresas devem estabelecer uma função de Responsável pela Segurança, o qual, entre os demais deveres previstos no presente regulamento, é responsável:

a) Pela gestão da política de segurança;

b) Pela gestão do sistema de gestão de segurança;

c) Pela promoção do cumprimento pelas empresas das obrigações em matéria de segurança e integridade das redes e serviços ao abrigo do disposto na lei e no presente regulamento.

2 – As empresas que não estejam estabelecidas na União Europeia ou no Espaço Económico Europeu e que detenham ativos classificados nas classes A, B ou C devem assegurar que o seu Responsável pela Segurança se encontra aí domiciliado.

Artigo 21.º

Ponto de Contacto Permanente

1 – As empresas devem estabelecer uma função de Ponto de Contacto Permanente que assegure, numa disponibilidade contínua (24 horas por dia e sete dias por semana), a capacidade de iniciar e de receber um fluxo de informação de nível operacional e técnico entre a empresa e a ANACOM, nomeadamente para os seguintes efeitos:

a) Eficácia da resposta a incidentes de segurança com impacte a nível do setor ou para além deste, incluindo no suporte à continuidade da prestação dos serviços previstos na alínea *f)* do n.º 3 do Artigo 24.º, e que envolva a participação de várias empresas;

b) Articulação entre a ANACOM e a empresa para a obtenção de informação operacional ou técnica, na sequência de notificação de violação de

segurança ou perda de integridade com impacte significativo submetida por aquela ou por outra empresa;

c) Construção e atualização de informação de situação integrada no contexto de uma violação de segurança ou perda de integridade com impacte significativo ou da ativação do planeamento civil de emergência ou de plano de emergência da proteção civil;

d) Operacionalização dos procedimentos fixados no âmbito do planeamento civil de emergência ou de plano de emergência da proteção civil.

2 – As empresas devem assegurar que o Ponto de Contacto Permanente dispõe de meios de contacto principais e alternativos para a comunicação com a ANACOM em condições normais de funcionamento e nas situações extraordinárias previstas nos termos do Artigo 2.º.

3 – As empresas que detenham ativos classificados nas classes A ou B devem estabelecer uma função de Ponto de Contacto Alternativo, em local geograficamente distinto do local onde é assegurada a função de Ponto de Contacto Permanente, que tenha a capacidade de assegurar as funções do Ponto de Contacto Permanente em caso de falha deste ou de impossibilidade de ser contactado.

Artigo 22.º

Equipa de Resposta a Incidentes de Segurança

As empresas devem assegurar o acesso aos serviços de Equipa de Resposta a Incidentes de Segurança, dotada dos recursos e dos conhecimentos necessários a uma eficaz preparação contra os riscos, ameaças e vulnerabilidades e à resposta a incidentes de segurança que afetem os ativos classificados nas classes A, B ou C ou os ativos críticos para a continuidade do funcionamento das suas redes ou serviços.

Artigo 23.º

Dossier de Segurança

1 – As empresas devem compilar e manter atualizado um *Dossier* de Segurança, o qual inclui:

a) O Inventário de Ativos;

b) A Caracterização Geral de Segurança;

c) O Plano de Segurança;

d) O Relatório Anual de Segurança;

e) O Programa Anual de Exercícios e o respetivo relatório de execução;

f) A Proposta de Auditoria e o Relatório de Auditoria, nas versões aceites pela ANACOM, e o Plano de Correção de Não Conformidades.

2 – Os documentos previstos no número anterior devem integrar o *Dossier* de Segurança na sua versão atualizada e em todas as suas versões históricas dos últimos cinco anos.

3 – O *Dossier* de Segurança deve incluir o registo dos incidentes de segurança com maior impacte ocorridos nos últimos cinco anos, incluindo cópias de todas as notificações e divulgações realizadas ao abrigo do disposto no Título III.

4 – Para além do disposto nos números anteriores, o *Dossier* de Segurança deve ainda integrar a demais documentação relativa à segurança e integridade das redes e serviços, nomeadamente no que respeita à organização, às funções e responsabilidades, à capacidade técnica e a quaisquer sistemas, processos, planos, medidas e registos.

5 – Toda a documentação integrada no *Dossier* de Segurança deve ser assinada pelo Responsável pela Segurança.

TÍTULO III

Obrigações de notificação e de informação ao público

CAPÍTULO I

Obrigações de notificação

Artigo 24.º

Circunstâncias

1 – Para efeitos do disposto no artigo 54.º-B da Lei das Comunicações Eletrónicas, as empresas estão obrigadas a notificar a 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 a 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 presente artigo, 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 presente artigo, 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 presente artigo, 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 presente artigo, 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 presente artigo, 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 presente artigo, 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 presente artigo, 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 n.º 5 do presente artigo, desde que:

i) Tenha uma duração igual ou superior a uma hora;

ii) Afete um número de assinantes ou de acessos igual ou superior a 1.000 ou, nos termos da alínea *e)* do n.º 4 do presente artigo, 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 pelos seus clientes, que impacte no funcionamento das redes e serviços através dos quais sejam prestados serviços relevantes à sociedade e aos cidadãos, por parte dos seus clientes, de natureza pública ou privada, de âmbito nacional ou regional, previstas no n.º 6 do presente artigo, desde que tenha uma duração igual ou superior a 30 minutos;

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 n.º 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 é 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) 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 n.º 3 e sem prejuízo da identificação pela 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;

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 n.º 3 e sem prejuízo da identificação pela ANACOM de outras entidades, devidamente notificadas às empresas com uma antecedência mínima de cinco dias úteis, considera-se como clientes relevantes:

a) O SIRESP – Sistema Integrado de Redes de Emergência e Segurança de Portugal;

b) A RNSI – Rede Nacional de Segurança Interna;

c) O SRPCBA – Serviço Regional de Proteção Civil e Bombeiros dos Açores;

d) A partir da data da notificação da sua identificação, pela ANACOM, às empresas:

i) Os operadores de serviços essenciais a identificar no âmbito da aplicação do diploma de transposição da Diretiva (UE) n.º 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União;

ii) Os proprietários ou operadores de infraestruturas críticas designadas ao abrigo do disposto no Decreto-Lei n.º 62/2011, de 9 de maio, e na demais legislação aplicável.

Artigo 25.º

Formato e Procedimentos

1 – Por cada violação de segurança ou perda de integridade que deva ser objeto de notificação ao abrigo do disposto no Artigo 24.º, as empresas devem submeter à ANACOM:

a) Uma notificação inicial, nos termos dos n.os 4 e 5 do presente artigo;

b) Uma notificação final, nos termos do n.os 8 e 9 do presente artigo;

c) Sempre que exigida, em conformidade com o disposto no n.º 6 do presente artigo, uma notificação de fim de violação de segurança ou perda de integridade com impacte significativo, nos termos dos n.os 6 e 7 do presente artigo.

2 – Na circunstância prevista na alínea *c)* do n.º 3 do Artigo 24.º, as empresas apenas devem submeter à ANACOM uma notificação final nos termos previstos nos n.os 8 e 9 do presente artigo, com as devidas adaptações.

3 – Na circunstância prevista na alínea *g)* do n.º 3 do Artigo 24.º, pode ser dirigida à ANACOM uma única série de notificações, nos termos previstos no n.º 1 do presente artigo, desde que as mesmas:

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

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 Artigo 24.º 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 da ANACOM;

b) Data e hora do início ou, em caso de impossibilidade de o determinar, da deteção da violação de segurança ou perda de integridade;

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

d) 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;

e) 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;

f) 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;

g) 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 à 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;

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

8 – A notificação final deve ser assinada pelo Responsável pela Segurança e enviada no prazo de 20 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) Identificador único da violação de segurança ou perda de integridade atribuído pela ANACOM aquando da notificação inicial;

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

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

d) 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 *b)* e *c)*;

e) 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), com indicação, onde aplicável, do respetivo identificador único no Inventário de Ativos, 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;

v) Área geográfica afetada, em km2;

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

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

h) 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;

i) 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;

j) 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;

k) Outra informação relevante;

l) Observações.

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

a) Acidente ou desastre natural;

b) Erro humano;

c) Ataque malicioso;

d) Falha de *hardware* ou de *software*; ou

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

11 – A informação incluída nas notificações previstas no presente artigo 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 à ANACOM.

12 – As notificações previstas no presente artigo 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 endereço de correio eletrónico e do número de telefone publicados no sítio institucional da ANACOM na *Internet*;

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 n.º 3 do Artigo 24.º, para a respetiva notificação.

14 – Tendo em vista o cabal cumprimento do disposto no presente Capítulo, 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 Artigo 24.º.

CAPÍTULO II

Obrigações de informação ao público

Artigo 26.º

Condições

1 – Para efeitos do disposto na alínea *b)* do artigo 54.º-E da Lei das Comunicações Eletrónicas, as empresas devem informar 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 2 – do presente artigo, 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 presente artigo, 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 presente artigo, 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 presente artigo, 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 presente artigo, 1.500 km2 > área geográfica afetada ≥ 1.000 km2)

2 – 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 é 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) 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.

3 – O disposto no presente artigo não prejudica que, em circunstâncias não previstas no n.º 1 – e sempre que o também considere de interesse público, a 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.

Artigo 27.º

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 Artigo 26.º, 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;

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 à ANACOM, 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) Manter a informação disponibilizada através da *Internet* acessível ao público, nas mesmas localizações referidas na alínea *b)*, durante o período de 20 dias úteis a contar da data do fim da violação de segurança ou perda de integridade.

2 – As empresas devem comunicar à ANACOM, logo que iniciem a sua atividade, os endereços URL 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 cinco dias úteis relativamente à sua execução.

3 – Tendo em vista o cabal cumprimento do disposto no presente Capítulo II, 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 Artigo 26.º.

TÍTULO IV

Auditorias à segurança das redes e serviços

CAPÍTULO I

Disposições gerais

Artigo 28.º

Dever de realização de Auditoria

Para efeitos do disposto nos n.os 1 e 2 do artigo 54.º-F da Lei das Comunicações Eletrónicas, as empresas que detenham ativos classificados nas classes A, B ou C devem assegurar a realização, por auditoras e a expensas suas, de auditorias à segurança das suas redes e serviços, nos termos previstos no presente Título IV.

Artigo 29.º

Âmbito

As empresas devem assegurar que as Auditorias permitem verificar, em relação aos ativos das classes A, B e C e aos ativos críticos para o funcionamento das suas redes e serviços e tendo em consideração a situação existente na empresa, o cumprimento das normas legais e regulamentares aplicáveis.

Artigo 30.º

Normas de referência

1 – As empresas devem assegurar que as Auditorias são realizadas em conformidade com as normas, especificações ou recomendações europeias e internacionais existentes sobre a matéria.

2 – Para efeitos do disposto no número anterior e até ao dia 30 de junho de cada ano, a ANACOM publica, no seu sítio institucional na *Internet,* as referências das normas, especificações e recomendações a que devem conformar-se as Auditorias do ano seguinte.

Artigo 31.º

Auditoras

1 – As Auditoras e todos os seus colaboradores envolvidos na realização das Auditorias devem cumprir os seguintes requisitos:

a) Competência técnica, nomeadamente de acordo com as normas, especificações e recomendações identificadas ao abrigo do disposto no n.º 2 do artigo anterior;

b) Experiência relevante no setor das comunicações eletrónicas, nomeadamente em matéria de planeamento, de operação ou de segurança e integridade das redes e serviços;

c) Credenciação adequada emitida pelas autoridades competentes para acesso a matéria classificada, sempre que necessário e nos termos legalmente previstos.

2 – As empresas devem assegurar que as Auditoras não são seus fornecedores para outros serviços que não sejam a realização de auditorias externas e independentes e que entregam declarações de inexistência de conflitos de interesses em seu nome e em nome de todos os colaboradores envolvidos.

Artigo 32.º

Dever de colaboração

1 – As empresas devem prestar às Auditoras toda a colaboração e assistência necessárias para a realização das Auditorias nos termos previstos no presente Título IV, nomeadamente:

a) Colaboração na preparação e na realização das Auditorias;

b) Colaboração na elaboração dos Relatórios de Auditoria;

c) Disponibilização de acesso a todos os meios de prova solicitados;

d) Disponibilização de acesso aos meios necessários, nomeadamente para a realização de testes;

e) Disponibilização de acesso aos locais;

f) Disponibilização de acesso aos fornecedores relevantes ao nível da segurança e integridade das redes e serviços;

g) Disponibilização de acesso aos colaboradores com funções de administração, direção ou gestão relacionadas com a segurança e integridade das redes e serviços.

2 – As empresas devem assegurar o acesso, por parte da ANACOM, aos seus fornecedores e colaboradores previstos nas alíneas *f)* e *g)* do número anterior, bem como a sua disponibilidade para a realização de reuniões com a ANACOM e para a prestação dos esclarecimentos que esta Autoridade lhes solicite.

CAPÍTULO II

Procedimentos de Auditoria

Artigo 33.º

Fases

As empresas devem assegurar que as Auditorias se realizam de forma faseada e sequenciada, incluindo a Fase de Pré-auditoria, a Fase de Auditoria e a Fase de Pós-auditoria, nos termos previstos no presente Capítulo II.

Artigo 34.º

Fase de Pré-auditoria

1 – As empresas devem elaborar, em conjunto com a Auditora, e apresentar à ANACOM uma Proposta de Auditoria que contenha os seguintes elementos:

a) Identificação da Auditora e de todos os seus colaboradores envolvidos em cada fase da Auditoria;

b) Identificação dos seus fornecedores relevantes ao nível da segurança e integridade das redes e serviços;

c) Identificação de todos os seus colaboradores com funções de administração, direção ou gestão relacionadas com a segurança e integridade das redes e serviços;

d) Comprovativos ou declarações que permitam atestar o cumprimento dos requisitos previstos no Artigo 31.º;

e) Plano de Correção das Não Conformidades da última Auditoria realizada, quando aplicável;

f) Programa da Auditoria, devidamente fundamentado, incluindo os seguintes elementos:

i) Data prevista para o início da Fase de Auditoria;

ii) Duração estimada da Fase de Auditoria;

iii) Indicação dos ativos abrangidos pela Auditoria, com referência aos respetivos identificadores únicos;

iv) Atividades previstas.

2 – As empresas devem apresentar à ANACOM a Proposta de Auditoria, assinada pelo Responsável pela Segurança:

a) No caso da primeira Auditoria, no prazo de 20 dias úteis a contar da data a partir da qual a empresa detenha um ativo classificado nas classes A, B ou C;

b) No caso das Auditorias seguintes, no prazo de dois anos a contar da data de apresentação da Proposta de Auditoria em que se baseou a Auditoria anterior ou, se posterior, no prazo de 20 dias úteis a contar da data em que a empresa volte a deter um ativo classificado nas classes A, B ou C.

3 – Compete à ANACOM proceder à aceitação da Proposta de Auditoria, podendo, para o efeito, solicitar à empresa a prestação dos esclarecimentos necessários e o suprimento de deficiências existentes.

Artigo 35.º

Fase de Auditoria

1 – As empresas devem iniciar a Fase de Auditoria no prazo máximo de 40 dias úteis a contar da data de aceitação, pela ANACOM, da Proposta de Auditoria.

2 – As empresas devem comunicar, com uma antecedência mínima de 20 dias úteis, as datas e locais em que as atividades da Fase de Auditoria se irão realizar, de modo a que a ANACOM possa, caso assim o entenda, assistir às mesmas.

3 – As empresas devem assegurar que a Auditora elabora um Relatório de Auditoria que, em conformidade com a Proposta de Auditoria aceite pela ANACOM, inclua os seguintes elementos:

a) Lista de não conformidades da situação existente na empresa em relação às normas de referência previstas no Artigo 30.º;

b) Descrição sintética das atividades desenvolvidas, incluindo:

i) Análise de documentação;

ii) Realização de entrevistas;

iii) Realização de testes;

iv) Verificação de funcionamento de equipamentos e de sistemas;

v) Simulação de procedimentos;

vi) Visitas aos locais;

c) Descrição da Fase de Auditoria, tendo em consideração os resultados das Análises do Risco realizadas;

d) Tempo total utilizado na Fase de Auditoria, discriminando o tempo gasto:

i) Na avaliação das Análises do Risco;

ii) Na análise de documentação;

iii) Na realização de entrevistas;

iv) Na realização de testes;

v) Na verificação de funcionamento de equipamentos e de sistemas;

vi) Na simulação de procedimentos;

vii) Nas visitas aos locais;

viii) Na elaboração do Relatório da Auditoria;

ix) Noutras atividades.

4 – As empresas devem enviar à ANACOM cópia do Relatório da Auditoria, assinado em nome da Auditora e, dele tomando conhecimento, pelo Responsável pela Segurança, no prazo de 10 dias úteis a contar da conclusão das atividades da Fase de Auditoria.

5 – Compete à ANACOM a aceitação do Relatório de Auditoria, podendo, para o efeito, solicitar à empresa a prestação dos esclarecimentos necessários e o suprimento de deficiências existentes.

Artigo 36.º

Fase de Pós-auditoria

1 – As empresas devem elaborar e enviar à ANACOM um Plano de Correção das Não Conformidades constantes do Relatório de Auditoria, assinado pelo Responsável pela Segurança, no prazo de 20 dias úteis a contar da data de aceitação, pela ANACOM, do Relatório de Auditoria.

2 – O Plano de Correção das Não Conformidades deve conter:

a) Identificação de todas as Não Conformidades e observações constantes do Relatório de Auditoria, incluindo eventuais conclusões e recomendações;

b) Em relação a cada Não Conformidade:

i) Uma análise das suas causas;

ii) A indicação das medidas de correção e dos respetivos prazos de execução.

3 – As empresas devem assegurar que cada uma das medidas constantes do Plano de Correção das Não Conformidades, referidas na alínea *b)* do número anterior, é executada logo que possível e que todas são executadas dentro do prazo máximo que a ANACOM, caso assim o entenda, venha a determinar.

TÍTULO V

Disposições finais e transitórias

Artigo 37.º

Regime sancionatório

As infrações ao disposto no presente regulamento são puníveis nos termos previstos nas alíneas *ee)*, *ff)* e *gg)* do n.º 2 e nas alíneas *u)*, *v)*, *x)* e *z)* do n.º 3 do artigo 113.º da Lei das Comunicações Eletrónicas.

Artigo 38.º

Entrada em vigor e disposições transitórias

1 – O presente regulamento entra em vigor no dia seguinte à data da respetiva publicação em Diário da República, sem prejuízo do disposto nos números seguintes.

2 – As empresas em atividade à data de entrada em vigor do presente regulamento devem:

a) No prazo de 40 dias úteis a contar da data de entrada em vigor do presente regulamento, estabelecer a função de Responsável pela Segurança, nos termos previstos no Artigo 20.º, comunicando à ANACOM, dentro do mesmo prazo, os elementos previstos na alínea *h)* do n.º 1 e no n.º 2 do Artigo 17.º;

b) No prazo de 80 dias úteis a contar da data de entrada em vigor do presente regulamento, estabelecer a função de Ponto de Contacto Permanente, nos termos previstos no Artigo 21.º, comunicando à ANACOM, dentro do mesmo prazo, os elementos previstos na alínea *i)* do n.º 1 e no n.º 2 do Artigo 17.º;

c) No prazo de um ano a contar da data de entrada em vigor do presente regulamento:

i) Classificar os ativos, elaborar o Inventário de Ativos e realizar uma Análise dos Riscos de âmbito global, nos termos previstos, respetivamente, nos Artigo 7.º, Artigo 8.º e Artigo 9.º, cumprindo, a partir de então, as demais obrigações aí previstas;

ii) Estabelecer, quando aplicável, a função de Ponto de Contacto Alternativo, nos termos previstos no Artigo 21.º, comunicando à ANACOM, dentro do mesmo prazo, os elementos previstos na alínea *i)* do n.º 1 e no n.º 2 do Artigo 17.º;

d) No prazo de 18 meses a contar da data de entrada em vigor do presente regulamento:

i) Adotar, quando aplicável, os procedimentos de controlo da gestão excecional de tráfego de acesso à *Internet*, nos termos previstos no Artigo 11.º;

ii) Adotar os procedimentos de gestão de alterações, nos termos previstos no Artigo 12.º;

iii) Adotar um sistema de controlo de acessos, nos termos previstos no Artigo 13.º;

iv) Adotar um sistema de monitorização e controlo, nos termos previstos no Artigo 14.º;

v) Elaborar e enviar à ANACOM a Caracterização Geral da Segurança, nos termos previstos no Artigo 17.º;

vi) Elaborar um Plano de Segurança, nos termos previstos no Artigo 18.º;

vii) Assegurar o acesso aos serviços de Equipa de Resposta a Incidentes de Segurança, nos termos previstos no Artigo 22.º;

viii) Compilar um Dossier de Segurança, nos termos previstos no Artigo 23.º;

e) Elaborar um Relatório Anual de Segurança, nos termos previstos no Artigo 19.º, a reportar ao 1.º ano civil seguinte ao ano civil da data de entrada em vigor do presente regulamento;

f) Elaborar e executar um programa anual de exercícios, nos termos previstos no Artigo 15.º, para o 2.º ano civil seguinte ao ano civil da data de entrada em vigor do presente regulamento;

g) No prazo de três anos a contar da data de entrada em vigor do presente regulamento, adotar as medidas de redundância, de robustez e de resiliência, nos termos previstos no Artigo 10.º.

3 – As empresas em atividade à data de entrada em vigor do presente regulamento que se encontrem abrangidas pelo dever de realização de Auditoria, ao abrigo do disposto no Artigo 28.º, devem apresentar à ANACOM uma Proposta de

Auditoria, nos termos previstos no Artigo 34.º, no prazo de dois anos a contar da referida data de entrada em vigor.

4 – As empresas que iniciem a sua atividade após a data de entrada em vigor do presente regulamento devem cumprir o disposto no n.º 2 e no n.º 3 nos prazos aí fixados ou, se posteriores, nos prazos fixados nos correspondentes artigos.

5 – O disposto no Artigo 16.º e no Título III entra em vigor no prazo de um ano a contar da data de entrada em vigor do presente regulamento.

Artigo 39.º

Norma revogatória

A decisão da ANACOM de 12 de dezembro de 2013 é revogada a partir do termo do prazo de um ano a contar da data de entrada em vigor do presente regulamento.