Regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas

A matéria da segurança e integridade das redes e serviços de comunicações eletrónicas foi introduzida na Lei das Comunicações Eletrónicas (Lei n.º 5/2004, de 10 de fevereiro, na sua atual redação) através da Lei n.º 51/2011, de 13 de setembro, em transposição da Diretiva 2002/21/CE do Parlamento Europeu e do Conselho de 7 de março de 2002 relativa a um quadro regulamentar comum para as redes e serviços de comunicações eletrónicas, alterada pela Diretiva 2009/140/CE, do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, tendo então sido cometidas à Autoridade Nacional das Comunicações (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 impacto 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 impacto 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 os requisitos aplicáveis às entidades auditoras, ao abrigo do disposto nos n.os 1 e 2 do artigo 54.º-F da Lei das Comunicações Eletrónicas.

Por decisão da ANACOM de 12 de dezembro de 2013, alterada em 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 impacto significativo no funcionamento das redes e serviços, tendo, a 12 de junho de 2014, entrado em atividade um centro de reporte, com funcionamento permanente, para a receção das notificações.

Tendo por base a experiência adquirida não só através da atividade do centro de reporte, mas também pela cooperação nacional e internacional nesta matéria, entendeu esta Autoridade dever exercer as competências acima referidas, através da aprovação de um regulamento relativo à segurança e integridade das redes e serviços.

No que respeita, em particular, às obrigações de notificação e de divulgação ao público, entendeu ainda esta Autoridade dever integrar neste regulamento o normativo correspondente 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, congregou-se e consolidou-se, num único instrumento, um conjunto devidamente articulado de condições aplicáveis em matéria de segurança e integridade das redes e serviços.

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 de um primeiro projeto de regulamento relativo à segurança e à integridade das redes e serviços, o qual, por decisão de 29 de dezembro de 2016, foi aprovado e submetido a procedimento regulamentar e procedimento geral de consulta, nos termos previstos no artigo 10.º dos Estatutos da ANACOM, aprovados pelo Decreto-Lei n.º 39/2015, de 16 de março, e nos 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.

Após publicação deste primeiro projeto na 2.ª série do *Diário da República*, a 10 de janeiro de 2017, e após prorrogação do prazo em 15 dias úteis, a consulta pública decorreu até ao dia 14 de março de 2017, tendo sido oportunamente recebidas 17 pronúncias.

Atentos os contributos recebidos e ponderada a natureza significativa das alterações introduzidas, nos termos fundamentados no relatório da consulta pública, entendeu a ANACOM dever proceder à elaboração de um segundo projeto de regulamento relativo à segurança e integridade das redes e serviços, o qual, por decisão de 6 de julho de 2018, foi aprovado e submetido a novo procedimento regulamentar e procedimento geral de consulta.

Após publicação deste segundo projeto na 2.ª série do *Diário da República*, a 22 de agosto de 2018, a consulta pública decorreu até ao dia 3 de outubro de 2018, tendo sido oportunamente recebidas 14 pronúncias, as quais foram devidamente consideradas na aprovação deste regulamento, constando a respetiva apreciação do relatório que fundamenta as opções da ANACOM e que se encontra publicado no sítio desta Autoridade, em conjunto com as pronúncias integrais recebidas.

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 impacto.

Para essa ponderação, contribuíram, em especial, as conclusões do estudo de avaliação e caracterização da segurança em redes de comunicações públicas, de 2010, e da avaliação da segurança e integridade das redes e serviços de comunicações eletrónicas a nível nacional, de 2012, ambos desenvolvidos pela ANACOM, bem como a informação e a experiência recolhida por esta Autoridade desde 2014, através do respetivo centro de reporte, no tratamento das notificações recebidas, no acompanhamento das violações de segurança ou perdas de integridade em causa e no âmbito da sua análise agregada, e da participação no Grupo de Peritos do Artigo 13.º-A, coordenado pela ENISA (Agência Europeia para a Segurança das Redes e da Informação).

Na sequência dos incêndios florestais ocorridos durante o ano de 2017, a ANACOM publicou um relatório de um grupo de trabalho que coordenou e que foi constituído por entidades públicas e privadas, designadamente a Associação Empresarial de Comunicações de Portugal (ACIST), a Autoridade Nacional de Proteção Civil (ANPC), a Associação dos Operadores de Comunicações Eletrónicas (APRITEL), a Direção-Geral de Energia e Geologia (DGEG), a Entidade Reguladora dos Serviços

Energéticos (ERSE), o Instituto de Telecomunicações (IT) e empresas dos sectores das comunicações eletrónicas, dos transportes e da energia.

Deste relatório, apresentado publicamente em sessão promovida pela ANACOM a 29 de maio de 2018, designado "*Relatório do Grupo de Trabalho dos Incêndios Florestais – Medidas de Proteção e Resiliência de Infraestruturas de Comunicações Eletrónicas"* e disponível no sítio institucional da ANACOM na Internet, constam 27 medidas que permitirão reduzir significativamente o impacto dos incêndios florestais nas redes e serviços de comunicações eletrónicas e, consequentemente, nos seus utilizadores e cuja implementação é, onde aplicável, devidamente articulada com o disposto neste regulamento.

Assim, no exercício das atribuições e poderes conferidos à ANACOM na alínea *m)* do n.º 1 e na alínea *e)* do n.º 2, ambos do artigo 8.º, na alínea *a)* do n.º 2 do artigo 9.º e no artigo 10.º, todos dos Estatutos da ANACOM, bem como nos artigos 2.º-A e 54.º-A a 54.º-D, na alínea *b)* do artigo 54.º-E, nos n.os 1 e 2 do artigo 54.º-F e no artigo 54.º-G da Lei das Comunicações Eletrónicas, e na prossecução e observância dos objetivos estabelecidos na alínea *c)* do n.º 1 e na alínea *f)* do n.º 4, ambos do artigo 5.º da mesma lei, o Conselho de Administração da ANACOM, no exercício das competências que lhe são conferidas pela alínea *b)* do n.º 1 do artigo 26.º dos Estatutos, aprovou, por decisão de 14 de março de 2019, o seguinte regulamento:

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 (Lei n.º 5/2004, de 10 de fevereiro, na sua atual redação) e nos termos previstos no Título II do presente regulamento;

b) As circunstâncias, o formato e os procedimentos aplicáveis às exigências de comunicação de violações de segurança ou perdas de integridade das redes com impacto 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 do presente regulamento;

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 impacto 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 do presente regulamento;

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 os requisitos aplicáveis às 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 do presente regulamento.

Artigo 2.º

Definições

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

a) «Ativos», 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 e os recursos conexos;

b) «Auditora», a entidade 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 28.º do presente regulamento;

c) «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;

d) «Centro principal de gestão e operação», o centro que, por defeito ou em modo alternativo, tem por função assegurar a gestão e a operação do funcionamento das redes e serviços e dos ativos, incluindo a identificação e resolução dos incidentes de segurança;

e) «Clientes relevantes», as entidades identificadas nos termos previstos no n.º 3 do presente artigo;

f) «Colaboradores», os trabalhadores ou os agentes das empresas;

g) «Colaboradores-chave», os colaboradores que desempenhem funções no domínio da gestão e da operação da segurança e integridade das redes e serviços de comunicações eletrónicas, incluindo, pelo menos:

i) O responsável da segurança, nos termos previstos no artigo 14.º;

ii) O adjunto do responsável da segurança, quando exista, nos termos previstos no artigo 14.º;

iii) Os colaboradores que assegurem a função de ponto de contacto permanente, nos termos previstos no artigo 15.º;

iv) Os colaboradores que integrem a equipa de resposta a incidentes de segurança, nos termos previstos no artigo 16.º;

h) «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;

i) «Incidente de segurança», o evento com um efeito adverso real na segurança das redes e serviços, incluindo uma violação de segurança ou perda de integridade;

j) «Nível de sofisticação 1», o nível básico, que inclui as medidas de segurança de base, nos termos previstos no artigo 7.º e no Anexo;

k) «Nível de sofisticação 2», o nível de norma de indústria, que inclui as medidas de segurança baseadas nas normas, especificações e recomendações nacionais, europeias e internacionais adequadas, incluindo a revisão da sua implementação, tendo em consideração

alterações técnicas ou organizacionais nas empresas ou incidentes de segurança, nos termos previstos no artigo 7.º e no Anexo;

l) «Nível de sofisticação 3», o nível de estado da técnica, que inclui as medidas de segurança avançadas, a monitorização contínua e a revisão estrutural da sua implementação tendo em consideração alterações técnicas ou organizacionais nas empresas, incidentes de segurança, testes ou exercícios, com vista a uma melhoria proativa da implementação das medidas de segurança, nos termos previstos no artigo 7.º e no Anexo;

m) «Responsável da segurança», o colaborador da empresa responsável pela gestão da segurança das redes e serviços e pela sua representação no exercício das funções que lhe são cometidas pelo presente regulamento, nomeadamente nos termos previstos no artigo 14.º;

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

o) «Serviços relevantes», os serviços relevantes à sociedade e aos cidadãos, prestados pelos clientes relevantes, nos termos previstos no n.º 4 do presente artigo;

p) «Violação de segurança ou perda de integridade com impacto significativo», a violação de segurança ou perda de integridade com o impacto previsto nos termos do artigo 21.º

2 – Para os efeitos do disposto no presente regulamento, são aplicáveis as seguintes siglas e acrónimos:

a) «ANACOM», a Autoridade Nacional de Comunicações (ANACOM);

b) «ANPC», a Autoridade Nacional de Proteção Civil;

c) «CNCS», o Centro Nacional de Cibersegurança;

d) «CNPD», a Comissão Nacional de Proteção de Dados;

e) «EMGFA», o Estado-Maior-General das Forças Armadas;

f) «ENISA», a Agência Europeia para a Segurança das Redes e da Informação;

g) «GNS», o Gabinete Nacional de Segurança;

h) «ICNF», o Instituto da Conservação da Natureza e das Florestas, I.P.;

i) «IPMA», o Instituto Português do Mar e da Atmosfera, I.P.;

j) «LCE», a Lei das Comunicações Eletrónicas;

k) «PASP», os Postos de Atendimento de Segurança Pública (Centros de Atendimento do 112);

l) «RNSI», a Rede Nacional de Segurança Interna;

m) «SIRESP», o Sistema Integrado de Redes de Emergência e Segurança de Portugal;

n) «SRPCBA», o Serviço Regional de Proteção Civil e Bombeiros dos Açores.

3 – Para os efeitos previstos na alínea *e)* do n.º 1, considera-se como clientes relevantes:

a) As entidades responsáveis pela gestão, exploração e manutenção do SIRESP, quanto ao funcionamento deste sistema;

b) O Ministério da Administração Interna, quanto ao funcionamento da RNSI;

c) O SRPCBA, quanto ao funcionamento da rede integrada de telecomunicações de emergência da Região Autónoma dos Açores;

d) O EMGFA, quanto ao funcionamento dos sistemas de informação e tecnologias de informação e comunicação necessários ao exercício do comando e controlo nas Forças Armadas;

e) O GNS, quanto ao funcionamento do CNCS;

f) Os operadores de serviços essenciais identificados nos termos previstos na Lei n.º 46/2018, de 13 de agosto, que estabelece o regime jurídico da segurança do ciberespaço, quanto à prestação de serviços essenciais;

g) 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, quanto à operação das infraestruturas críticas.

4 – Para os efeitos previstos na alínea *o)* do n.º 1, considera-se como serviços relevantes, os serviços que nos termos dos pedidos dos clientes relevantes sejam identificados nos contratos celebrados com as empresas, relativamente a ofertas de redes e serviços que sejam essenciais para assegurar a continuidade da prestação daqueles serviços relevantes.

Artigo 3.º

Âmbito

1 – No cumprimento das suas obrigações em matéria de segurança e integridade das redes e serviços, previstas na lei e no presente regulamento, as empresas devem adotar as medidas de um modo adequado:

a) Às condições normais de funcionamento;

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

i) Incidente de segurança;

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

iii) Exceções previstas nas alíneas *a)*, *b)* e *c)* do n.º 3 do artigo 3.º do Regulamento (UE) 2015/2120 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015, que estabelece medidas respeitantes ao acesso à Internet aberta e que altera a Diretiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas e o Regulamento (UE) 531/2012 relativo à itinerância nas redes de comunicações móveis públicas da União;

iv) Acidente grave ou catástrofe, 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;

vi) Ativação de plano de emergência de proteção civil ou de plano no âmbito do planeamento civil de emergência do sector das comunicações, nos termos previstos nas disposições legais e regulamentares aplicáveis;

vii) Grave ameaça à segurança interna, incluindo as situações de ataques terroristas, 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 à evolução das condições climáticas e dos riscos de

desastre natural ou de outros fenómenos extremos, incluindo tempestades, deslizamentos de terras, inundações, ventos fortes, incêndios florestais, sismos e maremotos, nomeadamente, entre outros aspetos, no que respeita à escolha dos locais, dos equipamentos, dos materiais e das infraestruturas de alojamento e aos procedimentos de proteção e de preservação.

3 – Para efeitos do disposto no número anterior, as empresas devem ter em consideração:

a) A informação emitida pelas entidades competentes nacionais, europeias ou internacionais;

b) A Estratégia Nacional de Adaptação às Alterações Climáticas 2020, aprovada pela Resolução do Conselho de Ministros n.º 56/2015, de 30 de julho.

4 – As empresas devem cumprir as suas obrigações em matéria de segurança e integridade das redes e serviços, previstas na lei e no presente regulamento, em conformidade com as disposições respeitantes à segurança de matérias classificadas no âmbito nacional e no âmbito das organizações internacionais de que Portugal é parte.

5 – As empresas devem assegurar que todos os ativos que, independentemente da sua propriedade, suportem o funcionamento das suas redes ou dos seus serviços, incluindo os equipamentos terminais na medida em que se encontrem sob sua gestão, são abrangidos no cumprimento das suas obrigações em matéria de segurança e integridade das redes e serviços, previstas na lei e no presente regulamento.

6 – Ao abrigo do princípio da boa administração, a ANACOM utiliza a informação transmitida pelas empresas no âmbito do presente regulamento para a prossecução das suas atribuições nas matérias do planeamento de emergência da proteção civil e do planeamento civil de emergência no setor das comunicações.

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 das redes e serviços.

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

a) Ocorrência de um ou mais incidentes de segurança, em especial nos casos de causa raiz comum;

b) Riscos, ameaças ou vulnerabilidades comuns ou que potenciam um efeito em cascata;

c) 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;

d) Fornecimentos comuns de bens ou serviços por terceiros.

3 – Para efeitos do disposto no número anterior, a ANACOM partilha com as empresas a lista dos respetivos pontos de contacto permanente, mantida ao abrigo do disposto no artigo 15.º.

4 – Para efeitos do disposto no presente artigo, as empresas devem ainda cooperar, consoante adequado, através da realização de ações conjuntas, da celebração de acordos de assistência mútua ou da partilha de informação ou de conhecimento.

Artigo 5.º

Meios eletrónicos

1 – Todas as comunicações dirigidas à ANACOM no âmbito do presente regulamento, bem como o envio de informação, devem ser realizadas por meios eletrónicos, nos termos a determinar pela ANACOM, em conformidade com o disposto na lei e sem prejuízo do acesso aos seus serviços.

2 – A ANACOM mantém e gere a informação em matéria de segurança e integridade num sistema de informação seguro, em conformidade com as disposições respeitantes à segurança de matérias classificadas no âmbito nacional e no âmbito das organizações internacionais de que Portugal é parte.

TÍTULO II

Obrigações das empresas em matéria de segurança e integridade

CAPÍTULO I

Disposições gerais

Artigo 6.º

Obrigações das empresas

1 – Ao abrigo do disposto no artigo 54.º-A da LCE 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 impacto dos incidentes de segurança nas redes interligadas, a nível nacional e internacional, e nos utilizadores, devendo as mesmas ser adequadas aos riscos existentes tendo em conta o estado da técnica;

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 medidas técnicas e organizacionais e os requisitos adicionais adotados pelas empresas para cumprimento do disposto na lei e no presente regulamento devem:

a) Ser 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 atual redação;

b) Ser baseadas, na ausência das decisões previstas na alínea anterior, nas normas, especificações e recomendações nacionais, europeias e internacionais existentes sobre a matéria, nomeadamente:

i) NP ISO/IEC 27001:2013 (*Tecnologia de Informação – Técnicas de segurança – Sistemas de Gestão de Segurança da Informação – Requisitos*) e suas revisões;

ii) ISO/IEC 27001:2013 (*Information technology – Security techniques – Information security management systems – Requirements*) e suas revisões;

iii) ISO/IEC 27002:2013 (*Information technology – Security techniques – Code of practice for information security controls*) e suas revisões;

iv) ISO/IEC 27011:2016 ou Recomendação ITU-T X.1051 (04/2016) (*Information technology – Security techniques – Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations)* e suas revisões*;*

v) Recomendação ITU-T X.1053 (11/2017) (*Code of practice for information security controls based on ITU-T X.1051 for small and medium-sized telecommunication organizations*) e suas revisões;

vi) ISO/IEC 27005:2018 (*Information technology – Security techniques – Information security risk management*) e suas revisões;

vii) Recomendação ITU-T X.1055 (11/2008) (*Risk management and risk profile guidelines for telecommunication organizations*) e suas revisões;

viii) Recomendação ITU-T X.1056 (01/2009) (*Security incident management guidelines for telecommunications organizations*) e suas revisões;

ix) Recomendação ITU-T X.1057 (05/2011) (*Asset management guidelines in telecommunication organizations*) e suas revisões;

x) ISO 22301:2012 (*Societal security – Business continuity management systems – Requirements*) e suas revisões;

xi) Outra norma, especificação ou recomendação nacional, europeia ou internacional adequada;

c) Ter em consideração os documentos técnicos publicados pela 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 atual redação.

3 – As medidas técnicas e organizacionais e os requisitos adicionais adotados pelas empresas para cumprimento do disposto na lei e no presente regulamento devem ainda ter em consideração:

a) As recomendações formuladas pela ANACOM, nomeadamente quanto à concretização das medidas de segurança previstas no presente regulamento;

b) As instruções técnicas aplicáveis à construção ou ampliação de infraestruturas aptas, à utilização de infraestruturas aptas e à instalação de equipamentos e sistemas de redes de comunicações eletrónicas em infraestruturas aptas, fixadas ao abrigo do disposto no Decreto-Lei n.º 123/2009, de 21 de maio, na sua atual redação.

4 – As empresas devem assegurar que as medidas técnicas e organizacionais e os requisitos adicionais adotados para cumprimento do disposto na lei e no presente regulamento são mantidos atualizados.

Artigo 7.º

Medidas técnicas de execução e requisitos adicionais

1 – Para efeitos do disposto no artigo anterior e nos termos previstos no n.º 1 do artigo 54.º-C e no artigo 54.º-D da LCE, as empresas devem, nomeadamente, adotar todas as medidas de segurança incluídas nos níveis de sofisticação 1 e 2 para a prossecução de cada um dos 25 objetivos de segurança constantes do Anexo.

2 – Excetua-se do disposto no número anterior os casos em que, tendo por fundamento os resultados de uma avaliação dos riscos para a segurança das redes e serviços, realizada pelas empresas:

a) Uma adequada prossecução de um objetivo de segurança não exija, a título excecional e mediante autorização prévia da ANACOM na sequência de um pedido fundamentado apresentado para o efeito, o cumprimento de uma ou de várias medidas de segurança previstas no nível de sofisticação 2;

b) Uma adequada prossecução de um objetivo de segurança exija o cumprimento de uma ou de várias medidas de segurança previstas no nível de sofisticação 3.

3 – Para efeitos do disposto na alínea *a)* do número anterior, os pedidos devem ser instruídos com os seguintes elementos:

a) Indicação do objetivo de segurança;

b) Indicação da medida de segurança;

c) A avaliação dos riscos que fundamenta o pedido e que garante, mediante o cumprimento de outras medidas, uma adequada prossecução do objetivo de segurança em causa.

4 – Ficam dispensadas da autorização prévia prevista na alínea *a)* do n.º 2 as empresas que, no conjunto das suas ofertas, tenham um número de assinantes ou de acessos inferior a 1.000 e cujas ofertas não sejam essenciais para assegurar a continuidade da prestação de um serviço relevante, sem prejuízo da necessária avaliação dos riscos para a segurança das redes e serviços nos termos previstos no mesmo n.º 2.

5 – Para efeitos do disposto no artigo anterior, as medidas de segurança a adotar pelas empresas devem incluir, no mínimo, as seguintes medidas específicas, nos termos previstos no Capítulo II do presente Título:

a) Classificação de ativos e inventário de ativos, nos termos previstos, respetivamente, nos artigos 8.º e 9.º;

b) Revisão das avaliações dos riscos, nos termos previstos no artigo 10.º;

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

d) Exercícios, nos termos previstos no artigo 12.º;

e) Informação aos clientes relevantes, nos termos previstos no artigo 13.º;

f) Responsável da segurança, nos termos previstos no artigo 14.º;

g) Ponto de contacto permanente, nos termos previstos no artigo 15.º;

h) Equipa de resposta a incidentes de segurança, nos termos previstos no artigo 16.º;

i) Plano de segurança, nos termos previstos no artigo 17.º;

j) Deveres específicos de comunicação à ANACOM, nos termos previstos no artigo 18.º;

k) Relatório anual de segurança, nos termos previstos no artigo 19.º.

CAPÍTULO II

Medidas específicas

Artigo 8.º

Classificação de ativos

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

2 – Um ativo deve ser classificado na classe A se, em resultado de perturbação do seu funcionamento, o número de assinantes ou de acessos afetados possa ser igual ou superior a 100.000 ou a área geográfica afetada possa, nos termos do n.º 3 do presente artigo, ser igual ou superior a 2.000 km^2 ou, quando aplicável, abranger a totalidade do território de uma ilha da Região Autónoma dos Açores ou da Região Autónoma da Madeira.

3 – Para efeitos do disposto no número anterior, 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 – 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 100.000;

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 que seja essencial para assegurar a continuidade da prestação de serviços relevantes e que como tal seja identificada no âmbito do contrato celebrado com o cliente relevante em causa;

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

e) Os ativos que tenham sido identificados no âmbito do planeamento civil de emergência do sector das comunicações ou de um plano de emergência de proteção civil, nos termos previstos, respetivamente, no Decreto-Lei n.º 73/2012, de 26 de março e na alínea *e)* do n.º 2 do artigo 2.º-A da LCE.

5 – Um ativo deve ser classificado na classe B se, em resultado de perturbação do seu funcionamento, cause ou possa vir a causar um impacto negativo grave na segurança das redes e serviços, exceto quando, nos termos previstos nos números anteriores, deva ser classificado na classe A.

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

Artigo 9.º

Inventário de ativos

1 – As empresas devem elaborar e manter atualizado um inventário de todos os ativos classificados nas classes A ou B, assinado pelo responsável da segurança.

2 – Para cada ativo, deve constar do inventário de ativos a seguinte informação:

a) Identificador único;

b) Designação;

c) Classificação, ao abrigo do disposto no artigo 8.º;

d) As coordenadas geográficas da sua localização;

e) A identificação das entidades detentoras ou gestoras dos locais;

f) Caracterização, incluindo:

i) Funcionalidades e serviços suportados;

ii) Fundamentação da classificação, ao abrigo do disposto no artigo 8.º, incluindo uma descrição do impacto potencial de uma perturbação do seu funcionamento;

iii) Identificação como ponto de falha única;

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) No caso de interligação, indicação do tipo (interligação internacional, interligação entre as Regiões Autónomas, interligação entre o Continente e uma Região Autónoma ou interligação entre ilhas na Região Autónoma dos Açores ou na Região Autónoma da Madeira) e identificação das empresas interligadas;

g) Medidas, controlos e registos de segurança adotados, incluindo as medidas de redundância, robustez e resiliência no caso de ativo identificado como ponto de falha única ao abrigo do disposto na subalínea *iii)* da alínea anterior;

h) Registo das violações de segurança ou perdas de integridade com impacto significativo ocorridas;

i) Registo das alterações efetuadas, incluindo os resultados dos testes de integração e de sistema realizados e os planos de restauro dos ativos.

3 – As empresas devem concluir o inventário de ativos no prazo de 60 dias úteis a contar da data de início de atividade.

4 – As empresas cujas ofertas se suportem em, pelo menos, um ativo classificável na classe A devem comunicar à ANACOM a lista dos ativos constantes do inventário, que, em relação a cada ativo, contenha a informação constante das alíneas *a)* a *d)* e da subalínea *ii)* da alínea *f)*, todas do n.º 2 do presente artigo:

a) Na sua versão inicial, no prazo de 60 dias úteis a contar da data de início de atividade ou, se posterior, da data a partir da qual as empresas suportem as suas ofertas num ativo classificável na classe A;

b) Numa versão atualizada, em conjunto com o relatório anual de segurança.

Artigo 10.º

Revisão das avaliações dos riscos

As empresas devem rever as avaliações dos riscos tendo em consideração, nomeadamente:

a) As violações de segurança ou perdas de integridade com impacto significativo ou quaisquer outras situações extraordinárias referidas na alínea *b)* do n.º 1 do artigo 3.º ocorridas nos dois anos anteriores;

b) A informação sobre ameaças, vulnerabilidades e riscos, incluindo os riscos resultantes da evolução das condições climáticas e os riscos de desastre natural ou de outros fenómenos extremos, emitida pelas entidades competentes nacionais, europeias ou internacionais, incluindo a ANPC, o IPMA, o ICNF e a ENISA, bem como a informação publicada anualmente ou comunicada às empresas pela ANACOM.

Artigo 11.º

Procedimentos de Controlo da Gestão Excecional de Tráfego de Acesso à Internet

1 – A adoção de medidas de gestão de tráfego de acesso à Internet pelas empresas deve respeitar o disposto no Regulamento (UE) 2015/2120 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015.

2 – As empresas devem registar a informação relevante para o controlo das medidas de gestão excecional de tráfego de acesso à Internet, que, em relação a cada medida adotada, inclui, 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) 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 e manter atualizado um sistema para a monitorização do tráfego de acesso à Internet, de modo contínuo, para a deteção:

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

b) De congestionamentos iminentes da rede.

Artigo 12.º

Exercícios

1 – As empresas devem elaborar e implementar um programa de exercícios, para um período máximo de dois anos, para avaliação da segurança das redes e serviços e da adequação do plano de segurança, com vista à melhoria das medidas técnicas e organizacionais adotadas, tendo em consideração, quando aplicável:

a) Os ativos classificados nas classes A ou B;

b) O acesso aos serviços de emergência;

c) O suporte à continuidade da prestação dos serviços relevantes.

2 – As empresas devem promover, na medida do adequado, a participação de outras empresas ou de terceiros na execução do programa de exercícios.

3 – As empresas devem participar nos exercícios conjuntos que a ANACOM, nos termos a determinar, considere necessários.

Artigo 13.º

Informação aos clientes relevantes

Na sequência de incidentes de segurança com impacto na oferta de redes e serviços que seja essencial para assegurar a continuidade da prestação de serviços relevantes e que como tal seja identificada no âmbito do contrato celebrado com o cliente relevante em causa, as empresas devem comunicar-lhes as medidas adotadas ou a adotar com impacto para a prestação dos serviços relevantes em causa.

Artigo 14.º

Responsável da segurança

1 – As empresas devem designar um responsável da segurança, ao qual, entre os demais deveres previstos no presente regulamento, cabe:

a) A gestão da política de segurança;

b) A gestão do conjunto das medidas adotadas em matéria de segurança das redes e serviços ao abrigo do disposto na lei e no presente regulamento.

2 – As empresas podem designar um adjunto do responsável da segurança, a quem cabe exercer as funções do responsável da segurança em caso de ausência ou impedimento deste.

3 – As empresas que não estejam estabelecidas na União Europeia ou no Espaço Económico Europeu e cujas ofertas se suportem em, pelo menos, um ativo classificável na classe A devem assegurar que os colaboradores designados para as funções previstas no presente artigo se encontram domiciliados num Estado-Membro da União Europeia ou do Espaço Económico Europeu.

Artigo 15.º

Ponto de contacto permanente

1 – As empresas devem estabelecer uma função de ponto de contacto permanente, que deve assegurar a capacidade de iniciar e de receber um fluxo de informação de nível operacional e técnico entre a empresa e a ANACOM, garantindo, nomeadamente:

a) A eficácia da resposta a incidentes de segurança com impacto a nível do sector ou para além deste, incluindo no suporte à continuidade da prestação dos serviços relevantes, e que envolva a participação de várias empresas;

b) A 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 impacto significativo submetida por aquela ou por outra empresa;

c) A construção e atualização de informação de situação integrada no contexto de uma violação de segurança ou perda de integridade com impacto significativo ou da ativação de plano de emergência da proteção civil ou de plano no âmbito do planeamento civil de emergência do sector das comunicações;

d) A operacionalização dos procedimentos fixados no âmbito de um plano de emergência da proteção civil ou do planeamento civil de emergência do sector das comunicações;

e) O tratamento das determinações da ANACOM no sentido da informação ao público de violações de segurança ou perdas de integridade ocorridas nas suas redes e serviços, ao abrigo do disposto no n.º 3 do artigo 23.º;

f) A receção das instruções vinculativas emitidas ao abrigo do disposto no n.º 1 do artigo 54.º-G da LCE;

g) A articulação entre a ANACOM e a equipa de resposta a incidentes de segurança.

2 – As empresas devem ainda assegurar que a função de ponto de contacto permanente se encontra dotada dos meios necessários ao desenvolvimento das ações de cooperação e partilha de informação entre empresas, nos termos do disposto no artigo 4.º.

3 – As empresas devem assegurar a função de ponto de contacto permanente:

a) Numa disponibilidade contínua (24 horas por dia e sete dias por semana), quando as suas ofertas se suportem em, pelo menos, um ativo classificável na classe A;

b) Numa disponibilidade contínua (24 horas por dia e sete dias por semana) limitada a períodos de ativação, iniciados e terminados mediante comunicação da ANACOM, nos restantes casos.

4 – 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, nas situações extraordinárias referidas nas subalíneas *i)*, *ii)* e *iii)* da alínea *b)* do n.º 1 do artigo 3.º e, conforme adequado e nos termos das disposições legais e regulamentares aplicáveis, nas situações referidas nas restantes subalíneas.

Artigo 16.º

Equipa de resposta a incidentes de segurança

1 – As empresas cujas ofertas se suportem em, pelo menos, um ativo classificável na classe A devem dispor de uma 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 ou B.

2 – As empresas devem concluir a constituição da equipa prevista no número anterior no prazo de seis meses a contar da data a partir da qual suportem as suas ofertas num ativo classificável na classe A.

3 – A equipa a que se refere o presente artigo deve integrar o sistema de resposta a incidentes de segurança da informação, nos termos a determinar ao abrigo do disposto na alínea *d)* do n.º 2 do artigo 2.º-A da LCE.

Artigo 17.º

Plano de segurança

1 – As empresas devem elaborar e manter atualizado um plano de segurança, devidamente documentado e assinado pelo responsável da segurança, que contenha:

a) A política de segurança;

b) A descrição de todas as medidas adotadas em matéria de segurança das redes e serviços ao abrigo do disposto na lei e no presente regulamento, incluindo, quando aplicável e caso a caso, as referências às medidas e aos níveis de sofisticação em que as mesmas se enquadram, nos termos previstos no Anexo;

c) O registo e análise dos incidentes de segurança com maior impacto ocorridos nos últimos cinco anos, incluindo todas as violações de segurança ou perdas de integridade com impacto significativo;

d) A lista dos colaboradores-chave, incluindo a indicação da respetiva função.

2 – As empresas devem concluir a elaboração do plano de segurança no prazo de seis meses a contar da data de início da sua atividade.

3 – As empresas devem ainda instruir o plano de segurança com os comprovativos de que o responsável da segurança, o adjunto do responsável da segurança, quando exista, e os colaboradores que asseguram a função de ponto de contacto permanente se encontram devidamente mandatados, nos termos legalmente previstos, para representar a empresa no exercício das funções que lhe foram cometidas, nos termos previstos na lei e no presente regulamento.

Artigo 18.º

Deveres específicos de comunicação à ANACOM

1 – As empresas devem comunicar à ANACOM, no prazo de 20 dias úteis a contar do início da sua atividade:

a) A política de segurança, nos termos previstos no artigo anterior;

b) A informação relativa aos colaboradores designados para as funções de responsável da segurança e, sendo o caso, de adjunto do responsável da segurança, nos termos previstos no artigo 14.º;

c) A informação relativa ao ponto de contacto permanente, nos termos previstos no artigo 15.º.

2 – Para efeitos do disposto na alínea *b)* do número anterior, as empresas devem comunicar à ANACOM, em relação a cada colaborador, os seguintes elementos:

a) Nome;

b) Número(s) de telefone;

c) Endereço de correio eletrónico.

3 – Para efeitos do disposto na alínea *c)* do n.º 1, as empresas devem comunicar à ANACOM os seguintes elementos:

a) Número de telefone fixo;

b) Número de telefone móvel;

c) Endereço de correio eletrónico;

d) Contactos alternativos;

e) Endereço geográfico do local onde é assegurada a função;

f) Quando aplicável, elementos de contacto para ativação da função de ponto de contacto permanente, nos termos previstos na alínea *b)* do n.º 3 do artigo 15.º, incluindo número de telefone fixo, número de telefone móvel e endereço de correio eletrónico.

4 – Antes do termo do prazo previsto no n.º 1 do presente artigo e em caso de necessidade, as empresas devem assegurar que os contactos fornecidos no âmbito da comunicação prévia de início de atividade, ao abrigo do disposto no artigo 21.º da LCE, asseguram, a título provisório, a função prevista no artigo 15.º do presente regulamento.

5 – As empresas devem comunicar à ANACOM, previamente à sua implementação, qualquer alteração da informação fornecida ao abrigo do disposto no presente artigo.

Artigo 19.º

Relatório anual de segurança

1 – As empresas devem elaborar um relatório anual de segurança, que, de forma completa, mas sucinta e em relação ao ano civil a que se reporta, contenha os seguintes elementos:

a) Descrição sumária das principais atividades desenvolvidas em matéria de segurança das redes e serviços, com especial enfoque nos ativos classificados nas classes A ou B e na implementação do programa de exercícios;

b) Estatística trimestral de todos os incidentes de segurança não notificados, com indicação do número e do tipo dos incidentes;

c) Análise agregada dos incidentes de segurança com maior impacto, incluindo todas as violações de segurança ou perdas de integridade com impacto significativo, e respetivo tempo médio de recuperação;

d) Recomendações de atividades, incluindo exercícios conjuntos, de medidas ou de práticas de cooperação que promovam a melhoria da segurança das redes e serviços;

e) Questões identificadas e lições aprendidas na sequência dos incidentes de segurança;

f) Qualquer outra informação relevante.

2 – As empresas devem apresentar o relatório anual de segurança à ANACOM, assinado pelo responsável da segurança:

a) Quanto ao primeiro relatório anual de segurança:

i) Até ao último dia útil do mês de janeiro do ano civil seguinte ao primeiro ano civil de atividade, quando esta tenha início no primeiro semestre;

ii) Até ao último dia útil do mês de janeiro do segundo ano civil seguinte ao primeiro ano civil de atividade, quando esta tenha início no segundo semestre;

b) Quanto aos demais relatórios anuais de segurança, até ao último dia útil do mês de janeiro do ano civil seguinte aos quais os mesmos se reportam.

3 – Para efeitos do disposto na subalínea *ii)* da alínea *a)* do número anterior, o relatório anual de segurança deve abranger todo o período entre a data de início de atividade e o final do ano civil anterior.

4 – Para efeitos do disposto na alínea *b)* do n.º 1, a ANACOM pode definir uma taxonomia comum de tipos de incidentes de segurança a ser utilizada pelas empresas, bem como o formato em que a informação deve ser apresentada.

TÍTULO III

Obrigações de notificação e de informação ao público

CAPÍTULO I

Obrigações de notificação

Artigo 20.º

Âmbito das obrigações de notificação

1 – Para efeitos do disposto no artigo 54.º-B da LCE, as empresas estão obrigadas a notificar a ANACOM das violações de segurança ou perdas de integridade com impacto significativo no funcionamento das redes e serviços que oferecem, nos termos previstos no presente Capítulo I.

2 – O cumprimento das obrigações de notificação previstas no presente Capítulo I não prejudica, nem substitui, nomeadamente:

a) O cumprimento, por parte das empresas, das suas obrigações de notificação dos incidentes de segurança em causa às autoridades competentes, nomeadamente a ANPC, o Ministério Público, o CNCS, a CNPD e as autoridades regionais, locais e sectoriais, nos termos previstos nas disposições legais e regulamentares aplicáveis, nomeadamente no âmbito do planeamento civil de emergência do sector das comunicações, da proteção civil e da segurança interna;

b) As comunicações, por parte das empresas, às demais empresas envolvidas nos incidentes de segurança em causa, na medida necessária ao cumprimento do disposto no artigo 4.º e no n.º 15 do artigo 22.º

3 – Para efeitos do disposto na alínea *a)* do número anterior, no âmbito das suas atribuições e competências, nomeadamente em matéria de planeamento civil de emergência do sector das comunicações e de proteção civil, a ANACOM pode, em colaboração com as autoridades competentes, formular recomendações às empresas quanto à articulação entre os procedimentos de notificação em causa.

Artigo 21.º

Circunstâncias

1 – Para efeitos do disposto no artigo anterior, 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 impacto significativo na continuidade desse funcionamento, de acordo com as circunstâncias e as regras previstas nos números seguintes.

2 – Para efeitos do disposto nos números anteriores, as empresas devem notificar a ANACOM:

a) De qualquer violação de segurança ou perda de integridade cujo impacto 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 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 km^2)
≥ 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 km^2 > área geográfica afetada ≥ 2.000 km^2)
≥ 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 km^2 > área geográfica afetada ≥ 1.500 km^2)
≥ 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 km^2 > área geográfica afetada ≥ 1.000 km^2)
≥ 6 horas	10.000 > n.º de assinantes ou de acessos afetados ≥ 5.000 (ou, nos termos da alínea *e)* do n.º 3 do presente artigo, 1.000 km^2 > área geográfica afetada ≥ 500 km^2)
≥ 8 horas	5.000 > n.º de assinantes ou de acessos afetados ≥ 1.000 (ou, nos termos da alínea *e)* do n.º 3 do presente artigo, 500 km^2 > área geográfica afetada ≥ 100 km^2)

b) De qualquer violação de segurança ou perda de integridade que afete a entrega aos PASP, 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 impacto 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 4 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 3 do presente artigo, uma área geográfica igual ou superior a 100 km^2;

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 que sejam essenciais para assegurar a continuidade da prestação dos serviços relevantes e que como tal sejam identificados no âmbito do contrato celebrado com os seus clientes relevantes, desde que tenha uma duração igual ou superior a 30 minutos;

g) De qualquer violação de segurança ou perda de integridade cujo impacto 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, na sua atual redação, preencha uma das condições previstas na alínea *a)* e, na parte que remete para esta alínea, na alínea *c)*, ambas do presente n.º 2.

3 – Para efeitos do disposto no número anterior:

a) O impacto 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.

4 – Para os efeitos previstos na alínea *d)* do n.º 2 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 LCE e do n.º 3 do artigo 12.º do presente regulamento;

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

Artigo 22.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 anterior, 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 dos 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 impacto significativo, nos termos dos n.ºs 6 e 7 do presente artigo.

2 – Na circunstância prevista na alínea *c)* do n.º 2 do artigo anterior, 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 2 do artigo anterior, 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 impacto 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 impacto significativo, até uma

hora após a verificação da circunstância prevista no artigo anterior 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, começando, quando aplicável, pelo restabelecimento da oferta de redes e serviços essenciais para assegurar a continuidade da prestação dos serviços relevantes.

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 impacto significativo;

d) Data e hora em que a violação de segurança ou perda de integridade perdeu o impacto 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 impacto, em termos de:

i) Redes e serviços afetados;

ii) Acesso aos serviços de emergência;

iii) Número de assinantes ou de acessos afetados;

iv) Clientes relevantes afetados, quando aplicável;

v) Área geográfica afetada, em km^2;

g) Observações.

6 – Após a perda de impacto 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 impacto significativo.

7 – A notificação referida no número anterior deve 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;

c) Indicação dos concelhos onde houve assinantes, acessos ou área geográfica afetados;

d) Descrição da situação do impacto existente no momento do fim de impacto significativo, nomeadamente:

i) Redes e serviços ainda afetados;

ii) Número de assinantes ou de acessos ainda afetados;

iii) Clientes relevantes ainda afetados, quando aplicável;

iv) Área geográfica ainda afetada, em km^2;

v) Concelhos onde ainda existam assinantes, acessos ou área geográfica afetados;

vi) Tempos estimados para a recuperação total dos assinantes, acessos, clientes relevantes ou área geográfica ainda afetados.

8 – A notificação final deve ser assinada pelo responsável da 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 impacto 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 impacto significativo;

c) Data e hora em que a violação de segurança ou perda de integridade perdeu o impacto 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) Impacto 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, no caso de ativos classificados nas classes A ou B, do respetivo identificador único, 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 e serviço;

iv) Clientes relevantes afetados, quando aplicável;

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

vi) Área geográfica afetada, em km^2;

vii) Freguesias e respetivos concelhos onde houve assinantes, acessos ou área geográfica afetados;

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) Descrição da situação residual do impacto existente à data da notificação final, nomeadamente:

i) Redes e serviços ainda afetados;

ii) Número de assinantes ou de acessos ainda afetados;

iii) Clientes relevantes ainda afetados, quando aplicável;

iv) Área geográfica ainda afetada, em km^2;

v) Freguesias e respetivos concelhos onde ainda existam assinantes, acessos ou área geográfica afetados;

vi) Tempos estimados para a recuperação total dos assinantes, acessos, clientes relevantes ou área geográfica ainda afetados;

l) Quando seja o caso, indicação da apresentação de denúncia ao Ministério Público;

m) Outra informação relevante;

n) Observações.

10 – Nos casos em que exista uma situação residual do impacto existente à data da notificação final, descrita ao abrigo do disposto na alínea *k)* do número anterior, as empresas devem comunicar à ANACOM, logo que possível, a recuperação total dessa situação residual.

11 – 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 fenómeno natural;

b) Erro humano;

c) Ataque malicioso;

d) Manutenção ou falha de *hardware* ou de *software*;

e) Falha no fornecimento de bens ou serviços por terceiro.

12 – 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.

13 – As notificações previstas no presente artigo devem ser realizadas através dos seguintes meios:

a) Por meios eletrónicos, nos termos a determinar pela ANACOM ao abrigo do disposto no n.º 1 do artigo 5.º;

b) Adicionalmente e no que respeita à notificação inicial e à notificação de fim de violação de segurança ou perda de integridade com impacto significativo, por telefone através do número a indicar pela ANACOM.

14 – Qualquer alteração aos contactos previstos no número anterior deve ser comunicada às empresas e publicada no sítio institucional da ANACOM na Internet, com uma antecedência mínima de 20 dias úteis.

15 – As empresas cujas redes ou serviços sejam afetados no seu funcionamento pela mesma violação de segurança ou perda de integridade, devem cooperar entre si para a correta deteção e avaliação de impacto dessa violação de segurança ou perda de integridade e, no caso previsto na alínea *g)* do n.º 2 do artigo anterior, para a respetiva notificação.

16 – Tendo em vista o cabal cumprimento do disposto no presente Capítulo, as empresas devem implementar todos os meios e os procedimentos necessários à deteção, à avaliação do impacto e à notificação das violações de segurança ou perdas de integridade que preencham as circunstâncias previstas no artigo anterior.

CAPÍTULO II

Obrigações de informação ao público

Artigo 23.º

Condições

1 – Para efeitos do disposto na alínea *b)* do artigo 54.º-E da LCE, as empresas devem informar o público de qualquer violação de segurança ou perda de integridade cujo impacto 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 km^2)
≥ 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 km^2 > área geográfica afetada ≥ 2.000 km^2)
≥ 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 km^2 > área geográfica afetada ≥ 1.500 km^2)
≥ 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 km^2 > área geográfica afetada ≥ 1.000 km^2)

2 – Para efeitos do disposto no número anterior:

a) O impacto 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 a ANACOM também o considere de interesse público e assim o determine, ao abrigo do disposto na alínea *b)* do artigo 54.º-E da LCE, as empresas devam informar o público de violações de segurança ou perdas de integridade ocorridas nas suas redes e serviços.

Artigo 24.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 anterior, as empresas devem:

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

i) A indicação das redes e serviços afetados;

ii) A indicação da zona ou das zonas que, em resultado das violações de segurança ou das perdas de integridade ocorridas, se encontram afetadas, desagregada ao nível do concelho, se possível de modo gráfico sobre um mapa de Portugal;

iii) 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 seguidas após a notificação inicial à ANACOM;

d) Assegurar que a informação disponibilizada se mantém permanentemente atualizada, nomeadamente 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 – A ANACOM, caso considere adequado e com vista a facilitar o acesso, por parte do público, à informação relativa a violações de segurança ou perdas de integridade, pode divulgar, nomeadamente no seu sítio institucional na Internet, uma lista dos endereços URL previstos no número anterior.

4 – Tendo em vista o cabal cumprimento do disposto no presente Capítulo II, as empresas devem implementar todos os meios e os procedimentos necessários à deteção, à avaliação do impacto e à divulgação das violações de segurança ou perdas de integridade que preencham as circunstâncias previstas no artigo anterior.

TÍTULO IV

Auditorias à segurança das redes e serviços

CAPÍTULO I

Disposições gerais

Artigo 25.º

Dever de realização de auditoria

Para efeitos do disposto nos n.ºs 1 e 2 do artigo 54.º-F da LCE, as empresas cujas ofertas se suportem em, pelo menos, um ativo classificável na classe A devem assegurar a realização, através de auditoras independentes e a expensas suas, de auditorias à segurança das suas redes e serviços, nos termos previstos no presente Título IV.

Artigo 26.º

Âmbito

As empresas devem assegurar que as auditorias se enquadram num ciclo de melhoria contínua e permitem verificar, em relação a uma amostra adequada dos ativos classificados nas classes A ou B e tendo em consideração a situação existente na empresa, o cumprimento das normas legais e regulamentares aplicáveis.

Artigo 27.º

Documentos e normas de referência

As empresas devem assegurar que as auditorias são baseadas nas normas, especificações ou recomendações nacionais, europeias e internacionais existentes sobre a matéria, nomeadamente:

a) ISO/IEC 17021-1:2015 (*Conformity assessment – Requirements for bodies providing audit and certification of management systems – Part 1: Requirements*) e suas revisões;

b) ISO/IEC TS 17021-5:2014 *(Conformity assessment – Requirements for bodies providing audit and certification of management systems – Part 5: Competence requirements for auditing and certification of asset management systems)* e suas revisões;

c) ISO/IEC TS 17021-6:2014 *(Conformity assessment – Requirements for bodies providing audit and certification of management systems – Part 6: Competence requirements for auditing and certification of business continuity management systems)* e suas revisões;

d) ISO/IEC 27006:2015 (*Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems*) e suas revisões;

e) ISO/IEC 27007:2017 *(Information technology – Security techniques – Guidelines for information security management systems auditing)* e suas revisões*;*

f) ISO 19011:2018 (*Guidelines for auditing management systems*) e suas revisões;

g) Outra norma, especificação ou recomendação nacional, europeia ou internacional adequada.

Artigo 28.º

Auditoras

1 – As empresas devem assegurar que as auditoras e todos os colaboradores destas envolvidos na realização das auditorias cumprem os seguintes requisitos:

a) Competência técnica, nomeadamente de acordo com as normas, especificações e recomendações aplicáveis ao abrigo do disposto no artigo anterior;

b) Experiência relevante no sector das comunicações eletrónicas, nomeadamente em matéria de planeamento, de operação ou de segurança 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 sejam seus fornecedores para outros serviços, com exceção da 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, em conformidade com a legislação aplicável.

3 – As empresas devem, salvo exceções devidamente fundamentadas, assegurar a rotatividade na escolha das auditoras, de modo a que a mesma auditora não realize mais do que duas auditorias consecutivas.

Artigo 29.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, incluindo o plano de segurança, os relatórios anuais de segurança e, quando aplicável, o relatório de auditoria e o plano de correção das não conformidades da última auditoria realizada;

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

e) Disponibilização de acesso aos locais;

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

g) Disponibilização de acesso aos colaboradores-chave.

2 – As empresas devem assegurar o acesso direto, por parte da ANACOM, às auditoras e aos fornecedores e colaboradores previstos, respetivamente, 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.

3 – As empresas devem salvaguardar o acesso direto às auditoras e aos fornecedores previstos na alínea *f)* do n.º 1, por parte da ANACOM, nos contratos celebrados com os mesmos.

CAPÍTULO II

Procedimentos de auditoria

Artigo 30.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 31.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) Comprovativos ou declarações que permitam atestar o cumprimento dos requisitos previstos no artigo 28.º;

c) 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 amostra, com referência aos respetivos identificadores únicos;

iv) Atividades previstas.

2 – As empresas devem apresentar à ANACOM a proposta de auditoria, assinada pelo responsável da segurança:

a) No caso da primeira auditoria, no prazo de seis meses a contar da data a partir da qual a empresa suporte as suas ofertas num ativo classificável na classe A;

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 seis meses a contar da data em que

a empresa volte a suportar as suas ofertas num ativo classificável na classe A.

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

Artigo 32.º

Fase de auditoria

1 – As empresas devem iniciar a fase de auditoria no prazo máximo de 60 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 queira e com uma antecedência mínima de cinco dias úteis em relação à data de início das atividades, designar um seu colaborador, devidamente credenciado nos termos previstos na alínea *c)* do n.º 1 do artigo 28.º, para 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;

b) Descrição e duração das atividades desenvolvidas.

4 – As empresas devem:

a) Assegurar, nos contratos celebrados com as auditoras, que o relatório da auditoria é enviado pela auditora, em simultâneo, à empresa e à ANACOM, no prazo de 20 dias úteis a contar da conclusão das atividades da fase de auditoria;

b) Enviar à ANACOM cópia do relatório da auditoria, assinado, dele tomando conhecimento, pelo responsável da segurança, no prazo de 5 dias úteis a contar da sua receção.

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

Artigo 33.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 da segurança, no prazo de 40 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 subalínea *ii)* da alínea *b)* do número anterior, é executada logo que possível ou dentro do prazo máximo que a ANACOM, caso assim o entenda, venha a determinar.

TÍTULO V

Disposições finais e transitórias

Artigo 34.º

Regime sancionatório

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

Artigo 35.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 – Sem prejuízo do cumprimento do disposto nos artigos 54.º-A a 54.º-G da LCE, 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:

i) Aprovar a política de segurança, comunicando-a à ANACOM, dentro do mesmo prazo, nos termos previstos na alínea *a)* do n.º 1 do artigo 18.º, e dar início à elaboração do plano de segurança, nos termos previstos no artigo 17.º;

ii) Estabelecer a função de responsável da segurança, nos termos previstos no artigo 14.º, comunicando à ANACOM, dentro do mesmo prazo, os elementos previstos na alínea *b)* do n.º 1 e no n.º 2 do artigo 18.º;

b) No prazo de 60 dias úteis a contar da data de entrada em vigor do presente regulamento, classificar os ativos previstos nas alíneas *a)*, *b)* e *d)* do n.º 4 do artigo 8.º;

c) 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 15.º, comunicando à ANACOM, dentro do mesmo prazo, os elementos previstos na alínea *c)* do n.º 1 e no n.º 3 do artigo 18.º;

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

i) Caso aplicável, adotar os procedimentos de controlo da gestão excecional de tráfego de acesso à Internet, nos termos previstos no artigo 11.º;

ii) Concluir a classificação dos ativos e o inventário de ativos, nos termos previstos, respetivamente, nos artigos 8.º e 9.º, e enviar a versão inicial da lista prevista no n.º 4 do artigo 9.º;

iii) Adotar todas as medidas de segurança incluídas no nível de sofisticação 1 e aplicáveis nos termos previstos no Título II e no Anexo ao presente regulamento, sem prejuízo do disposto nos n.os 3 e 5 do presente artigo;

e) No prazo de dezoito meses a contar da data de entrada em vigor do presente regulamento e caso aplicável, concluir a constituição da equipa de resposta a incidentes de segurança, nos termos previstos no artigo 16.º;

f) No prazo de dois anos a contar da data de entrada em vigor do presente regulamento:

i) Adotar todas as restantes medidas de segurança aplicáveis nos termos previstos no Título II e no Anexo ao presente regulamento, sem prejuízo do disposto nos n.os 3 e 5 do presente artigo;

ii) Concluir a elaboração do plano de segurança, nos termos previstos no artigo 17.º.

3 – Sem prejuízo do cumprimento do disposto nos artigos 54.º-A a 54.º-G da LCE, as empresas em atividade à data de entrada em vigor do presente regulamento devem ainda:

a) Elaborar o primeiro 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;

b) Elaborar e executar o primeiro programa de exercícios, nos termos previstos no artigo 12.º, no 2.º ano civil seguinte ao ano civil da data de entrada em vigor do presente regulamento;

c) Caso se encontrem abrangidas pelo dever de realização de auditoria, ao abrigo do disposto no artigo 25.º, apresentar à ANACOM a primeira proposta de auditoria, nos termos previstos no artigo 31.º, no prazo de dois anos a contar da data de entrada em vigor do presente regulamento.

4 – Sem prejuízo do cumprimento do disposto nos artigos 54.º-A a 54.º-G da LCE, as empresas que iniciem a sua atividade após a data de entrada em vigor do presente regulamento devem cumprir o disposto nos n.os 2 e 3 do presente artigo, nos prazos aí fixados, ou, se posteriores, nos prazos fixados nos correspondentes artigos.

5 – O disposto no artigo 13.º e no Título III entra em vigor no prazo de um ano a contar da data de entrada em vigor do presente regulamento.

6 – Até à determinação pela ANACOM do meio eletrónico específico para cada comunicação e para cada envio de informação, para efeitos do disposto no n.º 1 do artigo 5.º, os mesmos são realizados através de entrega nos serviços ou de remessa pelo correio.

7 – No caso dos prestadores de serviços energéticos e tendo em consideração a interdependência sectorial, a entrada em vigor das disposições relativas ao restabelecimento prioritário da oferta de redes e serviços, nos termos previstos no n.º 4 do artigo 22.º e na alínea *b)* do Objetivo de Segurança n.º 19 do Anexo, depende da entrada em vigor de condições de cooperação e de tratamento prioritário às empresas, no âmbito das disposições legais e regulamentares aplicáveis no sector energético.

Artigo 36.º

Comissão de acompanhamento

1 – Para acompanhamento da aplicação do presente regulamento, é criada uma comissão com a seguinte missão:

a) Promoção da harmonização de medidas;

b) Promoção da cooperação;

c) Avaliação de riscos emergentes;

d) Partilha de informação e de conhecimento;

e) Análise de desafios para a segurança das redes e serviços.

2 – A comissão de acompanhamento é composta por:

a) Um representante da ANACOM;

b) Os responsáveis da segurança das empresas cujas ofertas se suportem em, pelo menos, um ativo classificado na classe A ou um seu representante;

c) Quando designados, dois representantes das empresas que não suportem as suas ofertas em ativos classificados na classe A.

3 – A designação dos representantes previstos na alínea *c)* do número anterior é feita em reunião dos interessados convocada pela ANACOM, para um mandato renovável de três anos.

4 – A comissão de acompanhamento é coordenada pelo representante da ANACOM e reúne, ordinariamente, pelo menos duas vezes por ano e, extraordinariamente, por iniciativa da ANACOM.

5 – Podem assistir às reuniões da comissão de acompanhamento outras entidades convidadas pela ANACOM quando a discussão e a análise de matérias específicas assim o justifique.

6 – O apoio técnico e logístico ao funcionamento da comissão de acompanhamento será prestado pela ANACOM.

Artigo 37.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.

ANEXO

Objetivos e medidas de segurança

(a que se refere o n.º 1 do artigo 7.º)

1 – **Política de segurança**

Estabelecer e manter uma política de segurança das redes e serviços adequada.

Níveis de sofisticação	**Medidas de segurança**
1 (Básico)	a) Definir, aprovar e manter uma política de segurança de alto nível que abranja a segurança das redes e serviços. b) Publicar e comunicar aos colaboradores-chave a política de segurança.
2 (Norma de indústria)	c) Definir, aprovar e manter uma política de segurança pormenorizada relativamente aos ativos classificados nas classes A ou B e a processos de negócio críticos. d) Publicar e comunicar a todos os colaboradores a política de segurança e de que forma esta afeta o seu trabalho. e) Rever a política de segurança na sequência de alterações ou de incidentes de segurança.
3 (Estado da técnica)	f) Rever a política de segurança periodicamente, tendo em consideração, nomeadamente, os incidentes de segurança anteriores, os resultados de testes e exercícios e os incidentes de segurança que afetem outras empresas similares no sector.

2 – **Governação e gestão dos riscos**

Estabelecer e manter um quadro adequado de governação e gestão dos riscos com vista a identificar, prevenir, gerir e reduzir os riscos para a segurança das redes e serviços.

Níveis de sofisticação	Medidas de segurança
1 (Básico)	a) Elaborar uma lista dos principais riscos para a segurança das redes e serviços, tendo em consideração as ameaças a que os ativos classificados nas classes A ou B possam estar sujeitos. b) Dar conhecimento aos colaboradores-chave dos principais riscos e do modo como são mitigados.
2 (Norma de indústria)	c) Estabelecer uma metodologia e ferramentas de gestão dos riscos, ao nível de normas de indústria, incluindo normas, especificações e recomendações nacionais, europeias e internacionais existentes sobre a matéria. d) Garantir que os colaboradores-chave utilizam a metodologia e as ferramentas de gestão dos riscos. e) Rever as avaliações dos riscos na sequência de alterações ou de incidentes de segurança. f) Garantir que os riscos residuais são aceites pela gestão.
3 (Estado da técnica)	g) Rever a metodologia e as ferramentas de gestão dos riscos periodicamente, tendo em consideração, nomeadamente, as alterações e os incidentes de segurança anteriores.

3 – **Funções e responsabilidades no domínio da segurança**

Estabelecer e manter uma estrutura adequada de funções e responsabilidades no domínio da segurança das redes e serviços.

Níveis de sofisticação	Medidas de segurança
1 (Básico)	a) Atribuir aos colaboradores funções e responsabilidades no domínio da segurança das redes e serviços.

	b) Garantir que os colaboradores em desempenho de funções no domínio da segurança das redes e serviços estão contactáveis no caso de incidentes de segurança.
2 (Norma de indústria)	c) Nomear os colaboradores para as funções no domínio da segurança das redes e serviços. d) Dar conhecimento aos colaboradores das funções no domínio da segurança das redes e serviços existentes na empresa e de quando devem as mesmas ser contactadas.
3 (Estado da técnica)	e) Rever regularmente a estrutura das funções e responsabilidades no domínio da segurança das redes e serviços, tendo em consideração, nomeadamente, as alterações e os incidentes de segurança anteriores.

4 – **Segurança nos contratos com terceiros**

Estabelecer e manter uma política de segurança para os contratos com terceiros, com vista a garantir que as dependências de terceiros não afetem negativamente a segurança das redes e serviços.

Níveis de sofisticação	**Medidas de segurança**
1 (Básico)	a) Incluir requisitos de segurança nos contratos com terceiros.
2 (Norma de indústria)	b) Definir, aprovar e manter uma política de segurança para os contratos com terceiros. c) Garantir que todas as prestações de serviços e todos os fornecimentos de bens por terceiros cumprem a política de segurança para os contratos com terceiros. d) Rever a política de segurança para os contratos com terceiros na sequência de alterações ou de incidentes de segurança. e) Mitigar os riscos residuais que os terceiros não enderecem.

3 (Estado da técnica)	f) Registar os incidentes de segurança relacionados com terceiros ou causados por estes. g) Rever regularmente a política de segurança para os contratos com terceiros, tendo em consideração, nomeadamente, as alterações e os incidentes de segurança anteriores.

5 – **Verificação de credenciais e de referências**

Assegurar uma adequada verificação de credenciais e de referências dos colaboradores envolvidos, na medida necessária para as suas funções e responsabilidades.

Níveis de sofisticação	**Medidas de segurança**
1 (Básico)	a) Verificar as referências profissionais dos colaboradores.
2 (Norma de indústria)	b) Verificar as credenciais e as referências dos colaboradores, na medida necessária e nos termos permitidos por lei. c) Definir, aprovar e manter uma política e procedimentos de verificação de credenciais e de referências.
3 (Estado da técnica)	d) Rever regularmente a política e os procedimentos de verificação de credenciais e de referências, tendo em consideração, nomeadamente, as alterações e os incidentes de segurança anteriores.

6 – **Conhecimento, formação e treino em matéria de segurança**

Assegurar que os colaboradores dispõem de conhecimentos suficientes e recebem formação e treino regulares em matéria de segurança das redes e serviços.

Níveis de sofisticação	Medidas de segurança
1 (Básico)	a) Disponibilizar aos colaboradores-chave formação, treino e materiais relevantes sobre questões relacionadas com a segurança das redes e serviços.
2 (Norma de indústria)	b) Implementar um programa de formação e treino, garantindo que os colaboradores-chave dispõem de conhecimentos de segurança das redes e serviços suficientes e atualizados. c) Organizar sessões de formação e treino e de sensibilização para os colaboradores sobre os temas de segurança das redes e serviços com importância para a empresa.
3 (Estado da técnica)	d) Rever periodicamente o programa de formação e treino, tendo em consideração, nomeadamente, as alterações e os incidentes de segurança anteriores. e) Testar e avaliar os conhecimentos sobre segurança das redes e serviços dos colaboradores.

7 – **Mudança de colaboradores**

Estabelecer e manter um procedimento adequado de gestão das mudanças de colaboradores ou das mudanças de funções e responsabilidades.

Níveis de sofisticação	Medidas de segurança
1 (Básico)	a) Após a mudança de colaboradores, cancelar direitos, cartões, equipamentos e outros recursos de acesso, no caso de já não serem necessários ou permitidos. b) Dar conhecimento aos novos colaboradores das políticas e dos procedimentos em vigor e prestar-lhes formação acerca dos mesmos.
2 (Norma de indústria)	c) Definir, aprovar e manter uma política e procedimentos sobre mudanças de colaboradores, tendo em consideração o

	cancelamento atempado de direitos, cartões e equipamentos de acesso. d) Definir, aprovar e manter uma política e procedimentos sobre a formação e o treino dos colaboradores nas suas novas funções e responsabilidades.
3 (Estado da técnica)	e) Verificar periodicamente se as políticas e os procedimentos são eficazes. f) Rever as políticas e os procedimentos, tendo em consideração, nomeadamente, as alterações e os incidentes de segurança anteriores.

8 – **Tratamento de violações**

Estabelecer e manter um procedimento disciplinar para os colaboradores em caso de violação de políticas de segurança das redes e serviços ou estabelecer um procedimento mais abrangente que inclua incidentes de segurança causados por violações de políticas de segurança das redes e serviços por parte dos colaboradores.

Níveis de sofisticação	**Medidas de segurança**
1 (Básico)	a) Responsabilizar os colaboradores por incidentes de segurança causados pelas violações das políticas, nomeadamente no âmbito do contrato de trabalho e nos termos permitidos por lei.
2 (Norma de indústria)	b) Estabelecer procedimentos de tratamento das violações das políticas cometidas por colaboradores.
3 (Estado da técnica)	c) Rever periodicamente o procedimento disciplinar, tendo em consideração, nomeadamente, as alterações e os incidentes de segurança anteriores.

9 – **Segurança física e ambiental**

Estabelecer e manter a segurança física e ambiental adequada dos ativos.

Níveis de sofisticação	**Medidas de segurança**
1 (Básico)	a) Impedir o acesso físico não autorizado aos ativos e criar controlos ambientais para proteção contra as situações de acesso não autorizado, furto, incêndio e inundação. b) Definir, aprovar e manter procedimentos de proteção e de preservação dos ativos de um modo adequado à evolução das condições climáticas e dos riscos de desastre natural ou de outros fenómenos extremos, incluindo tempestades, deslizamentos de terras, cheias, ventos fortes, incêndios florestais, sismos e maremotos.
2 (Norma de indústria)	c) Definir, aprovar e manter uma política relativa às medidas de segurança física e aos controlos ambientais. d) Implementar controlos físicos e ambientais ao nível de norma de indústria, incluindo normas, especificações e recomendações nacionais, europeias e internacionais existentes sobre a matéria.
3 (Estado da técnica)	e) Avaliar periodicamente a eficácia dos controlos físicos e ambientais. f) Rever a política relativa às medidas de segurança física e aos controlos ambientais, tendo em consideração, nomeadamente, as alterações e os incidentes de segurança anteriores.

10 – **Segurança dos fornecimentos**

Estabelecer e manter uma segurança adequada dos fornecimentos (incluindo, entre outros, infraestruturas de alojamento, circuitos alugados, energia elétrica e combustível).

Níveis de sofisticação	Medidas de segurança
1 (Básico)	a) Garantir a segurança dos fornecimentos.
2 (Norma de indústria)	b) Definir, aprovar e manter uma política de segurança dos fornecimentos críticos. c) Implementar medidas de segurança ao nível de norma de indústria, incluindo normas, especificações e recomendações nacionais, europeias e internacionais existentes sobre a matéria, com vista a assegurar a continuidade dos fornecimentos.
3 (Estado da técnica)	d) Implementar medidas de segurança ao nível do estado da técnica com vista a assegurar a continuidade dos fornecimentos. e) Rever regularmente a política e as medidas de segurança com vista a assegurar a continuidade dos fornecimentos, tendo em consideração, nomeadamente, as alterações e os incidentes de segurança anteriores.

11 – **Controlo de acesso aos ativos**

Estabelecer e manter controlos de acesso físico e lógico adequados aos ativos.

Níveis de sofisticação	Medidas de segurança
1 (Básico)	a) Possuir identificadores únicos para os utilizadores e para os sistemas, que devem ser autenticados antes de aceder aos serviços ou aos sistemas. b) Implementar mecanismos de controlos de acesso aos ativos, de modo a permitir apenas uma utilização autorizada.
2 (Norma de indústria)	c) Definir, aprovar e manter uma política e procedimentos de controlo de acesso aos ativos, abrangendo, nomeadamente, as

	funções, os direitos, as responsabilidades e os procedimentos para atribuição e cancelamento de direitos de acesso. d) Selecionar mecanismos de autenticação adequados, dependendo do tipo e do nível de acesso. e) Monitorizar o acesso aos ativos e dispor de um procedimento de aprovação de exceções e de registo de acessos indevidos.
3 (Estado da técnica)	f) Avaliar a eficácia da política e dos procedimentos de controlo de acessos e implementar verificações cruzadas dos mecanismos de controlo de acessos. g) Rever a política, os procedimentos e os mecanismos de controlo de acessos.

12 – **Integridade dos ativos**

Estabelecer e manter a integridade dos ativos e protegê-los contra vírus, códigos maliciosos e outro *software* malicioso que alterem ou possam alterar a sua segurança e funcionalidade.

Níveis de sofisticação	**Medidas de segurança**
1 (Básico)	a) Assegurar que o *software* dos ativos não é adulterado ou alterado, nomeadamente com recurso a controlos de introdução e a *firewalls*. b) Assegurar que a informação crítica de segurança (incluindo, entre outra, palavras-passe, segredos partilhados e chaves privadas) não é divulgada ou adulterada. c) Verificar a existência de *software* malicioso nos ativos.
2 (Norma de indústria)	d) Implementar medidas de segurança ao nível de norma de indústria, incluindo normas, especificações e recomendações nacionais, europeias e internacionais existentes sobre a matéria, disponibilizando uma defesa em profundidade contra a adulteração e alteração dos ativos.

3 (Estado da técnica)	e) Implementar controlos ao nível do estado da técnica para proteger a integridade dos ativos. f) Rever a eficácia das medidas de segurança para proteger a integridade dos ativos.

13 – **Procedimentos operacionais**

Estabelecer e manter procedimentos para a operação dos ativos classificados nas classes A ou B pelos colaboradores.

Níveis de sofisticação	**Medidas de segurança**
1 (Básico)	a) Estabelecer procedimentos e definir e alocar as responsabilidades para a operação dos ativos classificados nas classes A ou B.
2 (Norma de indústria)	b) Definir, aprovar e manter uma política de operação dos ativos que assegure que os ativos classificados nas classes A ou B sejam operados e geridos de acordo com os procedimentos predefinidos.
3 (Estado da técnica)	c) Rever a política e os procedimentos de operação dos ativos classificados nas classes A ou B, tendo em consideração, nomeadamente, as alterações e os incidentes de segurança.

14 – **Gestão de alterações**

Estabelecer procedimentos de gestão de alterações aos ativos classificados nas classes A ou B com vista a minimizar a probabilidade de incidentes de segurança.

Níveis de sofisticação	**Medidas de segurança**
1 (Básico)	a) Estabelecer e definir procedimentos de introdução de alterações aos ativos classificados nas classes A ou B.

2 (Norma de indústria)	b) Definir, aprovar e manter uma política e procedimentos de gestão de alterações, com vista a garantir que as alterações aos ativos classificados nas classes A ou B são sempre realizadas de acordo com um procedimento predefinido. c) Documentar os procedimentos de gestão de alterações e registar, para cada alteração, as etapas do procedimento seguido.
3 (Estado da técnica)	d) Rever regularmente os procedimentos de gestão de alterações, tendo em consideração, nomeadamente, as alterações e os incidentes de segurança anteriores.

15 – **Gestão dos ativos**

Estabelecer e manter procedimentos de gestão dos ativos e de controlo de configurações de modo a gerir a disponibilidade e a configuração dos ativos classificados nas classes A ou B.

Níveis de sofisticação	**Medidas de segurança**
1 (Básico)	a) Gerir os ativos classificados nas classes A ou B e as suas configurações.
2 (Norma de indústria)	b) Definir, aprovar e manter uma política e procedimentos de gestão dos ativos e de controlo de configurações.
3 (Estado da técnica)	c) Rever regularmente a política e os procedimentos de gestão dos ativos e de controlo de configurações, tendo em consideração, nomeadamente, as alterações e os incidentes de segurança anteriores.

16 – **Procedimentos de gestão de incidentes de segurança**

Estabelecer e manter procedimentos de gestão de incidentes de segurança e de reencaminhamento para os colaboradores adequados.

Níveis de sofisticação	**Medidas de segurança**
1 (Básico)	a) Garantir a disponibilidade e a preparação de colaboradores para a gestão e o tratamento de incidentes de segurança. b) Registar e tipificar todos os incidentes de segurança.
2 (Norma de indústria)	c) Definir, aprovar e manter uma política e procedimentos de gestão de incidentes de segurança.
3 (Estado da técnica)	d) Investigar os incidentes de segurança com maior impacto e elaborar relatórios finais de incidentes de segurança, incluindo a indicação das medidas adotadas e recomendações para mitigar a futura ocorrência de incidentes de segurança do mesmo tipo. e) Rever a política e os procedimentos de gestão de incidentes de segurança, tendo em consideração, nomeadamente, os incidentes de segurança anteriores.

17 – **Capacidade de deteção de incidentes de segurança**

Estabelecer e manter uma capacidade de deteção de incidentes de segurança, com vista a assegurar uma resposta célere, eficaz e ordenada aos incidentes de segurança.

Níveis de sofisticação	**Medidas de segurança**
1 (Básico)	a) Implementar processos ou sistemas para a deteção de incidentes de segurança.

2 (Norma de indústria)	b) Implementar processos ou sistemas e procedimentos ao nível de norma de indústria, incluindo normas, especificações e recomendações nacionais, europeias e internacionais existentes sobre a matéria, para a deteção de incidentes de segurança. c) Implementar processos ou sistemas e procedimentos para registar e reencaminhar os incidentes de segurança, o mais rapidamente possível, para os colaboradores com funções adequadas.
3 (Estado da técnica)	d) Rever regularmente os processos ou sistemas e os procedimentos para a deteção de incidentes de segurança, tendo em consideração, nomeadamente, as alterações e os incidentes de segurança anteriores.

18 – **Notificação e comunicação de incidentes de segurança**

Estabelecer e manter procedimentos adequados de notificação e comunicação de incidentes de segurança, tendo em consideração o disposto na lei.

Níveis de sofisticação	**Medidas de segurança**
1 (Básico)	a) Notificar e comunicar incidentes de segurança em curso ou finalizados a autoridades, a terceiros, a clientes e ao público, consoante aplicável ou necessário.
2 (Norma de indústria)	b) Definir, aprovar e manter uma política e procedimentos de notificação e comunicação de incidentes de segurança.
3 (Estado da técnica)	c) Avaliar notificações e comunicações de incidentes de segurança. d) Rever a política e os procedimentos de notificação e comunicação de incidentes de segurança, tendo em consideração, nomeadamente, as alterações e os incidentes de segurança anteriores.

19 – **Estratégia de continuidade e planos de contingência**

Estabelecer e manter planos de contingência e uma estratégia de continuidade do funcionamento das redes e serviços.

Níveis de sofisticação	**Medidas de segurança**
1 (Básico)	a) Implementar uma estratégia de continuidade do funcionamento das redes e serviços, tendo em consideração, nomeadamente, as situações extraordinárias previstas na alínea *b)* do n.º 1 do artigo 3.º b) Estabelecer procedimentos de restabelecimento prioritário da oferta de redes e serviços através dos quais os clientes relevantes prestam os seus serviços relevantes, nomeadamente nas situações extraordinárias previstas na alínea *b)* do n.º 1 do artigo 3.º
2 (Norma de indústria)	c) Definir, aprovar e manter planos de contingência para os ativos classificados nas classes A ou B, tendo em consideração, nomeadamente, as situações extraordinárias previstas na alínea *b)* do n.º 1 do artigo 3.º d) Monitorizar a ativação e a execução dos planos de contingência e registar os tempos de recuperação com indicação de conformidade ou desconformidade em relação aos planos.
3 (Estado da técnica)	e) Rever periodicamente a estratégia de continuidade do funcionamento das redes e serviços. f) Rever os planos de contingência, tendo em consideração, nomeadamente, as alterações e os incidentes de segurança anteriores.

20 – **Capacidades de recuperação de desastres**

Estabelecer e manter capacidades adequadas de recuperação de desastres para o restauro das redes e serviços no caso de desastres naturais ou de grandes

proporções e outros fenómenos extremos, tendo em consideração, nomeadamente, a evolução das condições climáticas e as situações extraordinárias previstas na alínea *b)* do n.º 1 do artigo 3.º.

Níveis de sofisticação	**Medidas de segurança**
1 (Básico)	a) Estabelecer planos e medidas para a recuperação e o restauro das redes e serviços no caso de desastres, tendo em consideração, nomeadamente, as situações extraordinárias previstas na alínea *b)* do n.º 1 do artigo 3.º
2 (Norma de indústria)	b) Definir, aprovar e manter uma política e procedimentos para a dotação com capacidades de recuperação de desastres, tendo em consideração, nomeadamente, as situações extraordinárias previstas na alínea *b)* do n.º 1 do artigo 3.º c) Dotar-se com capacidades de recuperação de desastres ao nível de norma de indústria, incluindo normas, especificações e recomendações nacionais, europeias e internacionais existentes sobre a matéria, ou garantir que as mesmas estão disponíveis através de terceiros, tendo em consideração, nomeadamente, as situações extraordinárias previstas na alínea *b)* do n.º 1 do artigo 3.º
3 (Estado da técnica)	d) Dotar-se com capacidades de recuperação de desastres ao nível do estado da técnica, com vista a mitigar o impacto de desastres, tendo em consideração, nomeadamente, as situações extraordinárias previstas na alínea *b)* do n.º 1 do artigo 3.º e) Rever regularmente as capacidades de recuperação de desastres, tendo em consideração, nomeadamente, as alterações, os incidentes de segurança anteriores, os resultados de testes e de exercícios e as situações extraordinárias previstas na alínea *b)* do n.º 1 do artigo 3.º

21 – **Políticas de monitorização e registo de eventos**

Estabelecer e manter sistemas e funções de monitorização e de registo de eventos relativos aos ativos classificados nas classes A ou B.

Níveis de sofisticação	**Medidas de segurança**
1 (Básico)	a) Implementar procedimentos de monitorização e de registo de eventos relativos aos ativos classificados nas classes A ou B.
2 (Norma de indústria)	b) Definir, aprovar e manter uma política e procedimentos de monitorização e de registo de eventos relativos aos ativos classificados nas classes A ou B. c) Implementar mecanismos de monitorização dos ativos classificados nas classes A ou B. d) Implementar mecanismos para a recolha e armazenamento de registos de eventos relativos aos ativos classificados nas classes A ou B.
3 (Estado da técnica)	e) Implementar mecanismos para a recolha e análise automáticas de registos de eventos relativos aos ativos classificados nas classes A ou B. f) Rever a política, os procedimentos e os mecanismos de monitorização e de registo de eventos relativos aos ativos classificados nas classes A ou B, tendo em consideração, nomeadamente, as alterações e os incidentes de segurança anteriores.

22 – **Exercícios de planos de contingência**

Estabelecer e manter políticas de teste e de exercício de planos de contingência e de redundância, sempre que necessário em colaboração com terceiros.

Níveis de sofisticação	**Medidas de segurança**

1 (Básico)	a) Realizar exercícios e testes dos planos de contingência e de redundância, com vista a assegurar que os sistemas e os processos funcionam e que os colaboradores estão preparados em caso de incidentes de segurança com grande impacto.
2 (Norma de indústria)	b) Elaborar e implementar um programa de exercícios regulares para testar planos de contingência e de redundância, utilizando cenários realistas e variáveis ao longo do tempo. c) Assegurar que as questões identificadas e as lições aprendidas em resultado dos exercícios são tratadas pelos colaboradores responsáveis e que os sistemas e os processos relevantes são atualizados em conformidade.
3 (Estado da técnica)	d) Rever o programa de exercícios, tendo em consideração, nomeadamente, as alterações e os incidentes de segurança anteriores. e) Envolver nos exercícios fornecedores e outros terceiros, nomeadamente outras empresas, parceiros de negócio ou clientes.

23 – **Teste dos ativos**

Estabelecer e manter políticas para testar os ativos, nomeadamente em caso de ligação a novos ativos.

Níveis de sofisticação	**Medidas de segurança**
1 (Básico)	a) Testar os ativos antes da sua utilização ou da sua ligação aos ativos em exploração.
2 (Norma de indústria)	b) Definir, aprovar e manter uma política e procedimentos para testar os ativos. c) Implementar ferramentas de teste automático.

3 (Estado da técnica)	d) Rever a política, os procedimentos e as ferramentas de teste dos ativos, tendo em consideração, nomeadamente, as alterações e os incidentes de segurança anteriores.

24 – **Avaliações de segurança**

Estabelecer e manter uma política adequada para a realização de avaliações de segurança das redes serviços.

Níveis de sofisticação	**Medidas de segurança**
1 (Básico)	a) Assegurar que os ativos classificados nas classes A ou B são regularmente objeto de avaliações de segurança das redes e serviços, incluindo verificações e testes, nomeadamente em caso de introdução de novos ativos e na sequência de alterações.
2 (Norma de indústria)	b) Definir, aprovar e manter uma política e procedimentos para avaliações de segurança das redes e serviços.
3 (Estado da técnica)	c) Avaliar a eficácia da política e dos procedimentos para avaliações de segurança das redes e serviços. d) Rever a política e os procedimentos para avaliações de segurança das redes e serviços, tendo em consideração, nomeadamente, as alterações e os incidentes de segurança anteriores.

25 – **Monitorização da conformidade**

Estabelecer e manter uma política relativa à monitorização da conformidade com os requisitos legais e regulamentares.

Níveis de sofisticação	**Medidas de segurança**
1 (Básico)	a) Monitorizar a conformidade com os requisitos legais e regulamentares.
2 (Norma de indústria)	b) Definir, aprovar e manter uma política e procedimentos relativos à monitorização e auditoria da conformidade.
3 (Estado da técnica)	c) Avaliar a política e os procedimentos relativos à monitorização e auditoria da conformidade. d) Rever a política e os procedimentos relativos à monitorização e à auditoria da conformidade, tendo em consideração, nomeadamente, as alterações e os incidentes de segurança anteriores.