Regulamento que configura Instrução técnica relativa à comunicação e informação referentes a pontos de contacto permanente, responsável de segurança, inventário de ativos, relatório anual e notificação de incidentes

Relatório de consulta pública

Janeiro de 2022

1. Enquadramento

Por decisão de 3 de novembro de 2021 ao abrigo do disposto na alínea c) do n.º 1 do artigo 2.º-A, no artigo 3.º e no n.º 4 do artigo 4.º do Decreto -Lei n.º 3/2012, de 16 de janeiro, na redação atual, que aprova a orgânica do Gabinete Nacional de Segurança, nos termos do n.º 5 do artigo 7.º da Lei n.º 46/2018, de 13 de agosto, que estabelece o regime jurídico da segurança do ciberespaço e ao abrigo das competências delegadas através da alínea a) do n.º 1 do Despacho n.º 8689/2021, de 23 de agosto, do diretor -geral do Gabinete Nacional de Segurança, publicado no Diário da República, 2.ª série, de 2 de setembro de 2021, no subdiretor -geral do Gabinete Nacional responsável pela coordenação do Centro Nacional de Cibersegurança, foi aprovado o início do procedimento de elaboração de um regulamento que configura Instrução técnica relativa à comunicação e informação referentes a pontos de contacto permanente, responsável de segurança, inventário de ativos, relatório anual e notificação de incidentes, bem como a publicitação do respetivo anúncio para efeito de consulta pública, nos termos previstos nos artigos 98.º a 101.º do Código do Procedimento Administrativo.

A consulta pública decorreu pelo período de 30 dias, tendo sido oportunamente recebidas as seguintes 13 pronúncias:

— Auditsafe;

— ANA – Aeroportos de Portugal;

— APRITEL – Associação dos Operadores de Comunicações Eletrónicas («APRITEL»);

— Câmara Municipal de Portimão;

— Caixa Geral de Depósitos («CGD»);

— EDP Energias de Portugal, S.A. («EDP»);

— E-REDES - Distribuição de Eletricidade, S.A. («E-REDES»);[1]

— Hospital Distrital de Figueira da Foz, EPE;

— Município de Palmela;

— Necho Tech Law;

— NOWO COMMUNICATIONS, S.A. e ONITELECOM Infocomunicações, S.A. («NOWO/ONI»);

— REN — Redes Energéticas Nacionais («REN»);

— Universidade de Aveiro.

Assim, o presente relatório contém referência às pronúncias recebidas e a apreciação global do CNCS, que reflete o seu entendimento sobre as mesmas e que fundamenta as opções tomadas tendo em vista a aprovação do regulamento que configura Instrução técnica relativa à comunicação e informação referentes a pontos de contacto permanente, responsável de segurança, inventário de ativos, relatório anual e notificação de incidentes («Instrução»).

A análise deste documento não dispensa a consulta das versões integrais das pronúncias referenciadas, que – quando seja o caso, na sua versão não confidencial – são disponibilizadas no sítio institucional do CNCS na Internet, em www.cncs.gov.pt em conjunto com o presente relatório.

2. Comentários gerais

Realça-se a título inicial comentário recebido salientando a importância da iniciativa do legislador de regulamentação do Regime Jurídico de Segurança do Ciberespaço: *A regulamentação do regime jurídico de segurança do ciberespaço constitui um importante desenvolvimento, com um potencial aumento do nível de segurança dos dados e da informação* (EDP, p. 2.). *A EDP congratula a iniciativa e o foco do legislador nos temas da cibersegurança, considerando que o projeto constitui uma importante, e muito aguardada, peça na regulação da cibersegurança* (EDP, p. 3.).

Destaca-se ainda o mote construtivo dos comentários recebidos ao projeto de regulamento e a participação dos interessados, com proveniência nos setores público e privado. É ainda de salientar a participação de várias entidades provenientes do setor das comunicações eletrónicas e do setor da Energia.

Como comentários gerais devem ainda ser referidos os seguintes apresentados pelas entidades participantes:

É referido pela EDP que não foi prevista prorrogação para implementação das obrigações que decorrem do Decreto-Lei n.º 65/2021, de 30 de julho quando a forma específica da respetiva implementação se encontra em discussão (EDP, p. 3). No mesmo sentido é referido pela entidade APRITEL que *a APRITEL considera essencial que seja efetuada a devida derrogação das Disposições Transitórias do Decreto-Lei n.º*

[1] Os comentários enviados pela entidade E-REDES foram classificados por esta entidade no grau de classificação de segurança CONFIDENCIAL, não sendo por isso transcritos ou referidos no presente relatório, nem juntos em anexo como documento integral, na respetiva versão original, para consulta.

65/2021, de 30 de julho (APRITEL, p. 6) *e que caso se mantenha a obrigação de envio a 31 de janeiro de 2022, a APRITEL entende que cumprimento desta obrigação só poderá ser conseguido mediante envio de uma versão simplificada deste inventário* (APRITEL, p. 7).

Posição do CNCS

É entendimento do CNCS que a forma normativa do Decreto-Lei n.º 65/2021, de 30 de julho, estabelece prazos cuja aplicação se mantém, sem condicionante referente à aprovação de regulamento considerando que as disposições do referido Decreto-Lei são exequíveis nos termos já previstos neste normativo.

Concorda-se com o envio inicial de uma versão simplificada do inventário de ativos, no prazo definido no Decreto-Lei n.º 65/2021, de 30 de julho, que poderá ser complementada com informação posterior a enviar pelas entidades.

Ainda relativamente à aplicação de prazos previstos no Decreto-Lei n.º 65/2021, de 30 de julho, é questionado pela APRITEL: *Quanto ao Relatório anual, embora os elementos exigidos à sua elaboração estejam desde já concretizados no artigo 8.º do Decreto-Lei n.º 65/2021, de 30 de julho salienta-se que as obrigações e regras definidas entram em vigor apenas em novembro e dezembro de 2021. (…) Assim sendo, a APRITEL sugere que o envio do primeiro relatório anual seja efetuado apenas em 2023, respeitando um período em que as regras do Decreto-Lei n.º 65/2021, de 30 de julho já estão em vigor há pelo menos um ano, e existe uma plena definição sobre as Instruções Técnicas emitidas pelo CNCS.* (APRITEL, p. 7).

Posição do CNCS

A disposição transitória prevista no artigo 22.º do do Decreto-Lei n.º 65/2021, de 30 de julho, estabelece que: (1) O primeiro relatório anual a que se refere a alínea a) do n.º 2 do artigo 8.º deve ser entregue até 31 de janeiro de 2022, sem prejuízo do disposto na subalínea ii) da alínea a) do n.º 2 do mesmo artigo; e que (2) A versão inicial do inventário de ativos a que se refere o artigo 6.º deve ser entregue em conjunto com o relatório anual referido no n.º 1 do artigo 22.º do mesmo normativo. Nestes termos existe uma compatibilização referente aos prazos para o envio inicial do relatório anual e do inventário de ativos, sem prejuízo dos prazos previstos nos artigos 6.º e 8.º do referido normativo, devendo ainda referir-se que apenas no caso de entidades cuja atividade tenha início após a publicação do Decreto-Lei n.º 65/2021, de 30 de julho se aplica o prazo previsto na alínea a) do n.º 3 do artigo 6.º do Decreto-Lei n.º 65/2021, de 30 de julho, sendo que, após a aplicação da referida disposição transitória, nos temos da alínea b) do n.º 3 do artigo 6.º, o inventário de ativos deve ser entregue numa versão atualizada, anualmente, em conjunto com o relatório anual a que se refere o artigo 8.º.

Também relativamente à aplicação de prazos a APRITEL indica: *Por fim, quanto à indicação do ponto de contacto permanente e do responsável de segurança, nos termos previstos pelos artigos 4.º e 5.º do Projeto de Regulamento, as mesmas deveriam ser efetuadas, nos termos da lei, 90 dias após a entrada em vigor do Decreto-Lei n.º 65/2021, de 30 de julho, ou seja, até ao passado dia 6 de dezembro de 2021. Dado que os artigos 2.º e 3.º das Instruções Técnicas estabelecem que esta comunicação deve ser enviada por correio eletrónico, mediante preenchimento e junção de um formulário, solicita-se a confirmação de que as entidades sujeitas a estas obrigações devem proceder ao reenvio dos elementos já notificados ao CNCS.* (APRITEL, p. 7).

Posição do CNCS

Entende-se que após a publicação da versão final do regulamento que configura Instrução Técnica, as entidades devem enviar a informação que seja requerida nos termos da referida versão final de Instrução Técnica, aplicando-se os prazos para o efeito previstos no Decreto-Lei n.º 65/2021, de 30 de julho.

Também como considerações gerais refira-se o comentário da EDP indicando que o projeto de regulamento não versa sobre o plano de segurança, considerando-se por isso que o CNCS deve emitir com a maior brevidade possível uma Instrução que verse sobre o plano de segurança relativamente a clarificação dos seguintes pontos: i) o formato e o nível de exigência/requisitos do plano; ii) nível de detalhe exigido na descrição de todas as medidas adotadas (EDP, p. 4).

Posição do CNCS

Relativamente ao plano de segurança, deve referir-se que os respetivos elementos constam dos termos estabelecidos no artigo 7.º do Decreto-Lei n.º 65/2021, de 30 de julho, devendo no plano de segurança constar assim os seguintes elementos:

a) A política de segurança, incluindo a descrição das medidas organizativas e a formação de recursos humanos;

b) A descrição de todas as medidas adotadas em matéria de requisitos de segurança e de notificação de incidentes;

c) A identificação do responsável de segurança;

d) A identificação do ponto de contacto permanente.

Note-se ainda que no caso de operadores de infraestruturas críticas poderá utilizar-se o plano de segurança previsto no artigo 10.º do Decreto-Lei n.º 62/2011, de 9 de maio.

Refira-se ainda que o plano de segurança deve ser elaborado e mantido atualizado nos termos do n.º 1 do artigo 7.º do pelas entidades no âmbito de aplicação do Decreto-Lei n.º 65/2021, de 3 de julho, não sendo previsto o envio deste documento ao CNCS.

Deve ainda ser referido que não consta do artigo 7.º do Decreto-Lei n.º 65/2021, de 30 de julho a previsão de aprovação de Instrução para especificação dos respetivos termos ou elementos a constar, devendo a respetiva elaboração ser realizada de acordo com

os termos indicados neste normativo. Refira-se ainda que se prevê no n.º 1 do artigo 7.º do Decreto-Lei n.º 65/2021, de 30 de julho que o plano de segurança seja assinado pelo responsável de segurança de cada organização, devendo assim cada organização assegurar as capacidades mínimas para a elaboração e atualização deste documento.

Refere ainda a EDP que o projeto de Regulamento tal como o Decreto-Lei utiliza conceitos vagos e indeterminados que devem ser concretizados (EDP, p. 4).

Posição do CNCS

Relativamente à utilização de conceitos vagos e indeterminados no projeto de regulamento e no Decreto-Lei 65/2021, de 30 de julho, deve referir-se primariamente que o teor do Decreto-Lei não se encontra em consulta pública, tendo esta sido realizada previamente à respetiva publicação em Diário da República. Deve ainda referir-se que no comentário da EDP são apenas concretizados como conceitos entendidos como vagos e indeterminados no projeto de regulamento para a respetiva apreciação pelo CNCS, os seguintes conceitos de ativos essenciais, de "dispositivo físico" e de ativos direta ou indiretamente acessíveis através da Internet, abordados posteriormente neste relatório no âmbito do artigo 4.º do projeto de Regulamento.

É também referido pela EDP que a aprovação de Instruções pelo CNCS deve ter em consideração outros normativos como o Regulamento Geral de Proteção de Dados e o Regime das Infraestruturas Críticas (EDP, p. 4 e 5).

Posição do CNCS

Deve ser referido que é entendimento do CNCS que as disposições constantes do Projeto de Regulamento que configura Instrução técnica relativa à comunicação e informação referentes a pontos de contacto permanente, responsável de segurança, inventário de ativos, relatório anual e notificação de incidentes, como normativo complementar ao Decreto-Lei n.º 65/2021, de 30 de julho, não prejudicam a aplicação do Regulamento Geral de Proteção de Dados e do Decreto-Lei 62/2011, de 9 de maio.

É ainda referido pela EDP que deve ser promovida a avaliação de equivalências entre normativos setoriais e a legislação referente ao regime jurídico de segurança do ciberespaço, em articulação com os reguladores e entidades com poderes de supervisão setoriais (EDP, p. 9).

Posição do CNCS

Deve referir-se a aplicação do artigo 18 (2) do Decreto-Lei n.º 65/2021, de 30 de julho, a realizar com as entidades reguladoras e entidades com poderes de supervisão setoriais, nos termos do qual sempre que um ato jurídico setorial da União Europeia exigir que as entidades abrangidas por este decreto-lei garantam a segurança das respetivas redes e dos respetivos sistemas de informação ou a notificação de incidentes, são aplicáveis as disposições desse ato jurídico setorial desde que os seus requisitos tenham pelo menos efeitos equivalentes às obrigações constantes do Decreto-Lei n.º 65/2021, de 30 de julho, devendo, sempre que necessário, ser especificada a respetiva implementação pelo CNCS em articulação com as entidades reguladoras e com as entidades com poderes de supervisão sobre os setores e subsetores identificados no anexo ao Regime Jurídico da Segurança do Ciberespaço, seguindo-se o seguinte procedimento:

a) O CNCS, em articulação com as entidades reguladoras e as entidades com poderes de supervisão sobre os setores e subsetores identificados no anexo ao Regime Jurídico da Segurança do Ciberespaço avaliam o grau de equivalência das regras relativas ao inventário de ativos e ao relatório anual bem como dos requisitos de segurança e notificação de incidentes estabelecidos para cada setor;
b) Na avaliação do grau de equivalência deve ser ponderado em que medida os requisitos setoriais definidos pela lei, pelas disposições europeias e pelos normativos setoriais cumprem os requisitos previstos no Decreto-Lei n.º 65/2021, de 30 de julho, procurando, sempre que possível, evitar a sobreposição de requisitos e reportes;
c) O CNCS emite, por instrução técnica, o resultado da avaliação do grau de equivalência prevista no Decreto-Lei n.º 65/2021, de 30 de julho.

Devem ainda referir-se as considerações da EDP referentes à indicação de que o regulamento em consulta pública deveria preparar as organizações para a revisão da Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho de 6 de julho de 2016 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União (EDP, p. 4).

Posição do CNCS

Deve referir-se que a revisão da Diretiva (UE) 2016/1148 se encontra em curso, não sendo plausível a aprovação de conteúdo para normativo de nível nacional tendo por base projeto de legislação da União Europeia, não consolidado na presente data e não publicado de acordo com a respetiva versão final.

Também como considerações gerais devem ser referidos os comentários da NOWO/ONI quando indicam que *no entendimento manifestado pela NOWO e ONI em anteriores oportunidades, defendeu-se que os requisitos de segurança e notificação no âmbito da Lei de Segurança do Ciberespaço, quando aplicados a empresas que também atuam no sector das Comunicações Eletrónicas, deverão aproveitar o mais possível o trabalho feito por essas empresas no âmbito do Regulamento SIRSCE* (NOWO/ONI, p. 1).

Posição do CNCS

Deve considerar-se que o setor das comunicações eletrónicas não fica no âmbito de aplicação da Lei n.º 46/2018, de 13 de agosto, nem do Decreto-Lei n.º 65/2021, de 30 de julho, não podendo indicar-se a título de legislação especial os normativos regulamentares do setor das comunicações eletrónicas, nos termos previstos no artigo 18 (2) do Decreto-Lei n.º 65/2021, de 30 de julho.

Em referência à estrutura do presente relatório, a mesma segue a ordem de articulado do projeto de Regulamento que configura Instrução técnica relativa à comunicação e informação referentes a pontos de contacto permanente, responsável de segurança, inventário de ativos, relatório anual e notificação de incidentes, com indicação dos comentários recebidos de cada entidade participante e a apreciação do CNCS, resultante na decisão final da versão a aprovar do regulamento.

3. Comentários específicos

3.1. Artigo 1.º

Relativamente ao artigo 1.º do projeto de Regulamento que configura Instrução técnica relativa à comunicação e informação referentes a pontos de contacto permanente, responsável de segurança, inventário de ativos, relatório anual e notificação de incidentes foram apresentados comentários pela Caixa Geral de Depósitos e pela Câmara Municipal de Portimão no sentido de o envio de informação ao CNCS ser obrigatoriamente cifrado: *Sugere-se que a informação enviada ao CNCS tenha de ser sempre cifrada, pelo menos, no que respeita aos operadores de serviços essenciais (setor bancário)* (CGD); no mesmo sentido é referido pela Câmara Municipal de Portimão: *no n.º 2 é deixada a hipótese de encriptar a informação a enviar, não seria mais prudente que esta fosse obrigatoriamente encriptada?*

É ainda indicado pela Câmara Municipal de Portimão no âmbito do referido artigo 1.º do projeto de Regulamento que: *A criação de formulários online que permitisse o envio "direto" de informação em https, não permitiria um grau de segurança e uniformização maior que o envio de emails não formatados*.

Também no âmbito do artigo 1.º do projeto de Regulamento é sugerido pela entidade Necho Tech Law o seguinte: *As comunicações a estabelecer entre as entidades e o CNCS deverão ser efetuadas de modo a: a) Garantir a autenticidade da entidade emissora; b) Garantir a integridade da informação transmitida ao CNCS.*

Posição do CNCS

Entende-se que a cifragem de informação é facultativa para utilização pelas entidades no âmbito do previsto nos artigos 1.º e 6.º do projeto de Regulamento, sendo fornecida chave criptográfica pelo CNCS para o efeito, disponível na página da Internet do CNCS.

Deve ainda considerar-se que poderão ser aprovadas Instruções setoriais, referentes aos setores no âmbito de aplicação do Decreto-Lei n.º 65/2021, de 30 de julho, nos termos do artigo 18.º do Decreto-Lei n.º 65/2021, de 30 de julho, referente à aprovação de instruções setoriais em matéria de requisitos de segurança e de notificação de incidentes e à avaliação de equivalência de normativos setoriais, com a colaboração das entidades reguladoras e com poderes de supervisão em setores específicos. Nestas Instruções poderá ser prevista por razões fundamentadas a obrigatoriedade de envio de informação cifrada ao CNCS. Deve ainda considerar-se que o carácter facultativo do envio de informação de modo cifrado pelas entidades sob supervisão serve um princípio de adequação à tipologia de entidades e informação remetida por cada entidade ao CNCS.

Deve ainda ser referido que nos termos dos artigos 2.º (3), 3.º (3), 4.º (4), 5.º (2), 6.º (1) do projeto de Regulamento, se encontra previsto o envio de informação ao CNCS através da utilização de formulários *on line* cuja utilização pode ser realizada através da página da Internet do CNCS. Deve ainda ser referido que se entende que o tratamento de informação nos termos indicados no n.º 3 do artigo 1.º do projeto de Regulamento, é o adequado para a salvaguarda da segurança de informação, de acordo com os termos do qual o CNCS mantém e gere a informação recebida, num sistema de informação seguro em conformidade com as disposições respeitantes à segurança de matérias classificadas com o grau de segurança Reservado na marca Nacional, salvo quando necessário grau de segurança superior.

Quanto à garantia da autenticidade das entidades e integridade da informação transmitida ao CNCS deve ser referido que os princípios da autenticidade da entidade emissora e da integridade da informação transmitida, serão garantidos com recurso a sistema de identificação eletrónico com nível de garantia «elevado», nos termos definidos pelos artigos 8.º e 9.º do Regulamento (UE) n.º 910/2014, do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança, designadamente através do Cartão de Cidadão e da Chave Móvel Digita, conforme previsto no n.4 do artigo 19.º Decreto-Lei n.º 65/2021, de 30 de julho.

3.2. Artigo 2.º

Relativamente ao artigo 2.º do projeto de regulamento é indicado pela entidade REN — Redes Energéticas Nacionais o seguinte: *A REN, à semelhança de outras empresas, possui um ponto de contacto permanente 24/7 que é suportado num atendimento do helpdesk. O helpdesk possui a lista das pessoas em escala de disponibilidade em caso de incidente e que entraria em contacto com o CNCS. Desta forma, sugere-se que o ponto de contacto permanente não seja necessariamente uma pessoa, podendo ser um serviço disponível 24/7.*

No mesmo sentido é indicado pela entidade NOWO/ONI o seguinte: *Assinala-se que os pontos de contacto permanente na NOWO e na ONI são assegurados por equipas de supervisão, cuja constituição é alterada com alguma frequência, por motivos operacionais. Assim, não operacionalmente adequado comunicar contactos de pessoas específicas como ponto de contacto permanente. (…) Assim, solicita-se que o nº 2 do*

artº 2º seja revisto de forma a permitir que seja designada uma equipa operacional como ponto de contacto permanente. (NOWO/ONI, p. 1 e 2).

É também indicado pela entidade ANA – Aeroportos de Portugal que a mesma entende dever haver um único ponto de contacto permanente e gestor de segurança para o conjunto de infraestruturas aeroportuárias geridas por esta entidade (ANA – Aeroportos de Portugal, p. 2).

É ainda questionado pela entidade Universidade de Aveiro no âmbito do artigo 2.º:

As funções definidas no nº1 do artº 4º do Dec. Lei Nº 65/2021 devem ser asseguradas por todos os elementos designados como ponto de contacto?
Ainda, no que respeita ao definido no nº2 do artº 4º do Dec. Lei Nº 65/2021, para melhor assegurar as funções do contacto permanente, podem clarificar o que se entende por "períodos de ativação" e se a disponibilidade referida é diferente e em que medida o é, durante as "24horas por dia e sete dias por semana" e durante os "períodos de ativação"?
No formulário do Anexo I, como deve ser indicada a lista de pessoas que asseguram o "Ponto de contato permanente"? (Universidade de Aveiro, p. 1).

Também no âmbito do artigo 2.º do projeto de Regulamento é indicado pela entidade EDP: *na medida em que é cada vez menos utilizada a comunicação por telefone fixo, a EDP sugere que esta informação seja de natureza meramente facultativa* (EDP, p. 5).

É ainda sugerido pela entidade Necho Tech Law a densificação da informação referente ao ponto de contacto permanente, com correspondência no Anexo I do projeto de Regulamento.

Posição do CNCS

Relativamente aos comentários apresentados pelas entidades REN e NOWO/ONI, foi entendido como pertinente integrar os mesmos de forma a facilitar o entendimento já veiculado por esta entidade no sentido de que o ponto de contacto permanente é entendido como uma função. Nestes termos foi aprovada a seguinte redação para o n.º 2 do artigo 2.º do projeto de Regulamento, com a mesma alteração em correspondência com o Anexo I do projeto de Regulamento:

2 — A informação a constar da comunicação a realizar ao CNCS deve conter o nome da pessoa ou pessoas responsáveis, ou serviço disponível ou equipa operacional, por assegurar as funções de ponto de contacto permanente, e indicação dos meios de contacto principais e alternativos, nomeadamente contendo, no mínimo, a seguinte informação

Deve ainda ser referido que não obstante a possibilidade de externalização do ponto de contacto permanente, por exemplo quando coincidente com a função de SOC ou SCIRT, se entende que o responsável de segurança, previsto no artigo 5.º do Decreto-Lei n.º 65/2021, de 30 de julho, deve ser interno às organizações tratando-se de uma posição a atribuir internamente, com responsabilidades na organização inerente ao desempenho desse cargo, nesse sentido se entende que o responsável de segurança não pode ser externalizado, sem prejuízo de serviços de consultoria que a entidade entenda adquirir por via externa.

Deve ainda ser referido que as entidades no âmbito de aplicação da Lei n.º 46/2018, de 13 de agosto e do Decreto-Lei n.º 65/2021, de 30 de julho são identificadas nos termos da tipologia prevista no artigo 2.º da referida Lei, para o qual remete o n.º 1 do artigo 2.º do Decreto-Lei n.º 65/2021, de 30 de julho, sendo assim as obrigações decorrentes do Decreto-Lei n.º 65/2021, de 30 de julho aplicadas de acordo com esta mesma tipologia. De acordo com a identificação prevista na Lei n.º 46/2018, de 13 de agosto, as entidades consideradas como operadores de serviços essenciais são definidas nos termos das alíneas g) e t) do artigo 3.º do mesmo normativo como uma entidade pública ou privada que presta um serviço essencial para a manutenção de atividades societais ou económicas cruciais, que dependa de redes e de sistemas de informação e em relação ao qual a ocorrência de um incidente possa ter efeitos perturbadores relevantes na prestação desse serviço.

Nestes termos, os operadores de serviços essenciais foram identificados com a colaboração das entidades reguladoras e com poderes de supervisão nos diferentes setores e subsetores de acordo com critérios aplicados setorialmente, tendo sido identificadas e formalmente notificadas as entidades que realizam serviços essenciais de acordo com a tipologia definida no anexo à Lei n.º 46/2018, de 13 de agosto. Com este enquadramento aplica-se o n.º 5 do artigo 3.º do Decreto-Lei n.º 65/2021, de 30 de julho, nos termos do qual as entidades referidas no n.º 1 do artigo 2.º deste normativo podem estabelecer formas de colaboração com vista ao cumprimento das obrigações em matéria de requisitos de segurança e de notificação de incidentes previstos no Regime Jurídico da Segurança do Ciberespaço, e no Decreto-Lei n.º 65/2021, de 30 de julho, numa lógica de partilha de recursos, desde que seja assegurada a efetiva operacionalização das mesmas em cada entidade, sem prejuízo da responsabilização de cada entidade individualmente considerada a que haja lugar pela infração a qualquer disposição do Decreto-Lei n.º 65/2021, de 30 de julho, nos termos do n.º 6 do respetivo artigo 3.º.

Relativamente à sugestão apresentada pela EDP relativa ao carácter facultativo da indicação de telefone fixo, foi entendido como pertinente reter esta sugestão, tendo em conformidade sido alterados os artigos 2.º (2), alíneas d) e f), do projeto de Regulamento com indicação “se aplicável”, e nos mesmos termos o artigo 3.º (2), alínea e), e os Anexos I e II do projeto de Regulamento.

Deve ainda ser esclarecido relativamente às questões apresentadas pela Universidade de Aveiro que de acordo com o artigo 4.º (1) do Decreto-Lei 65/2021, de 30 de julho, as entidades no âmbito de aplicação deste normativo devem indicar, pelo menos, um ponto de contacto permanente ao CNCS.

Note-se que de acordo com o artigo 4.º (2) do mesmo normativo, as entidades devem assegurar a função de ponto de contacto permanente com uma disponibilidade contínua de 24 horas por dia e de sete dias por semana, limitada a períodos de ativação, iniciados e terminados mediante comunicação do CNCS.

Neste sentido, a disponibilidade de 24 horas por dia deve ser aplicada de acordo com comunicação a realizar pelo CNCS às entidades, pelo período definido para o efeito, cessando após a decorrência deste período, ou seja, a disponibilidade contínua de 24 horas por dia é limitada como referido a períodos de ativação a comunicar pelo CNCS.

Deve ainda ser referido que nos termos do artigo 4.º (3) a função de ponto de contacto permanente pode ser exercida por uma pessoa ou por várias pessoas.

Deve também ser referido que o Anexo I ao projeto de Regulamento deve ser utilizado para indicar os elementos que identificam o ponto de contacto permanente, preenchendo os campos constantes do referido Anexo.

Refira-se ainda que não se entende como pertinente a obrigatoriedade de envio de informação adicional relativa ao ponto de contacto permanente, além da prevista no artigo 2.º do projeto de Regulamento e respetivo Anexo I.

3.3. Artigo 3.º

Relativamente ao artigo 3.º é sugerido pela entidade Auditsafe que: *as partes responsáveis pela comunicação e informação exigidas possam ser apoiadas também um representante de Segurança da Informação de uma empresa especializada em SI, com certificações (…).*

É também indicado pela EDP, da mesma forma que em referência ao artigo anterior, que *na medida em que é cada vez menos utilizada a comunicação por telefone fixo, a EDP sugere que esta informação seja de natureza meramente facultativa* (EDP, p. 6).

É ainda referido no âmbito do artigo 3.º pela Universidade de Aveiro que: *A leitura do Dec. Lei Nº 65/2021, conjugada com o definido nesta instrução técnica, faz equivaler a função do "responsável de segurança" ao CISO (Chief Information Security Officer) definido no Quadro Nacional de Referência em Cibersegurança. Se assim for, devia ser clarificado que se trata da mesma função. Caso contrário, devem ser definidas as diferenças de funções entre as duas figuras: o Responsável de Segurança e o CISO* (Universidade de Aveiro, p.1).

É ainda sugerido pela entidade Necho Tech Law a densificação da informação referente ao responsável de segurança, com correspondência no Anexo II do projeto de Regulamento.

Posição do CNCS

A forma normativa do projeto de regulamento não contempla, sob a forma regulamentar que configura Instrução técnica ao Decreto-Lei n.º 65/2021, de 30 de julho, a definição da gestão interna dos recursos humanos de cada entidade.

Como referido anteriormente deve ainda ser indicado que, não obstante a possibilidade de externalização do ponto de contacto permanente previamente indicada e que resulta na alteração do n.º 2 do artigo 2.º do projeto de Regulamento, se entende que o responsável de segurança, previsto no artigo 5.º do Decreto-Lei n.º 65/2021, de 30 de julho, deve ser interno às organizações, tratando-se de uma posição com responsabilidades na organização, inerente ao desempenho desse cargo. Nesse sentido se entende que o responsável de segurança não pode ser externalizado, sem prejuízo de serviços de consultoria e/ ou suporte que a entidade entenda adquirir por via externa.

Refira-se também novamente que, relativamente à sugestão apresentada pela EDP relativa ao carácter facultativo da indicação de telefone fixo, foi entendido como pertinente reter esta sugestão, tendo em conformidade sido alterados os artigos 2.º (2),

alíneas d) e f), do projeto de Regulamento com indicação "se aplicável", e nos mesmos termos o artigo 3.º (2), alínea e), e os Anexos I e II do projeto de Regulamento.

Relativamente à sugestão apresentada pela Universidade de Aveiro, deve ser referido que nos termos do artigo 5.º (1) do Decreto-Lei n.º 65/2021, de 30 de julho, as entidades devem designar um responsável de segurança para a gestão do conjunto das medidas adotadas em matéria de requisitos de segurança e de notificação de incidentes.
Deve também ser referido que a função de CISO é exercida na organização, para o que se estabelece uma relação contratual, com o objetivo de garantir a segurança da informação dessa mesma organização, não se encontrando como tal previsto no âmbito do Decreto-Lei n.º 65/2021, de 30 de julho, sem prejuízo de se entender que o CISO de uma entidade pode ser designado para as funções de responsável de segurança, ficando no âmbito de decisão da entidade a respetiva designação.

Deve ainda esclarecer-se que a função de CISO se encontra tipificada no Quadro Nacional de Referência para a Cibersegurança, no ponto 5.2. com a indicação das respetivas funções.

Refira-se ainda que não se entende como pertinente a obrigatoriedade de envio de informação adicional relativa ao ponto de contacto permanente, além da prevista no artigo 3.º do projeto de Regulamento e respetivo Anexo II.

3.4. **Artigo 4.º**

Relativamente ao artigo 4.º do projeto de Regulamento, é sugerido pela Caixa Geral de Depósitos: *a clarificação desta disposição no que respeita à inventariação dos ativos alojados em cloud.*

É também referido pela entidade Município de Palmela no âmbito do artigo 4.º do projeto de Regulamento: *consideramos que sendo os IP em questão dinâmicos, perderão rapidamente a atualidade, e que em relação ao endereço de hardware este será de difícil obtenção sem que tenhamos que recorrer a software específico para a sua inventariação (…). Face ao exposto, propomos que em 2022 o CNCS reavalie a necessidade de envio da informação relativa aos IP e aos endereços de hardware dos computadores pessoais e da informação necessária dos equipamentos ativos de rede e explicite junto das entidades visadas, em particular junto dos Municípios (…) as razões que presidem ao pedido de informação com elevado grau de detalhe e as formas mais ágeis para a obter*.

É também referido pela REN no âmbito do mesmo artigo: *Propõe-se que seja clarificado o que se entende por ativos indiretamente acessíveis. O entendimento feito relativamente a este ponto é que seriam todos os ativos / serviços acessíveis através de um, ou mais, endereços IPs públicos. Na al. iv do nº 3 do artº 4 é solicitado "Endereço IP". A informação relativa ao endereço IP pode variar dinamicamente com sistemas de balanceamento. Sugere-se que em complemento ou alternativamente sejam incluídos os FQDNs.*

São também feitas sugestões pelo Hospital Distrital de Figueira da Foz EPE, no sentido de serem incluídos mais elementos para identificação dos ativos utilizados por cada entidade e também sugestões para a análise de risco a realizar por cada entidade no âmbito do artigo 10.º do Decreto-Lei n.º 65/2021, de 30 de julho.

No mesmo sentido são realizadas propostas pela entidade Necho Tech Law no sentido de densificar os termos de classificação dos ativos utilizados por cada entidade.

É, no entanto, indicado pela Universidade de Aveiro relativamente ao artigo 4.º que: *Pretende-se perceber o objetivo do detalhe da lista de ativos a comunicar ao CNCS, em concreto: Se a informação pretende ter um cariz operacional/situacional, a sua comunicação deveria ser regular e por meios automatizados (API), atendendo às previsíveis mudanças nas infraestruturas de equipamentos e, essencialmente, de software. Tendo um objetivo de informação situacional, em princípio, os benefícios superam os riscos envolvidos na partilha. Se a informação pretende apenas ser demonstrativa da realização do inventário, será, em princípio, excessiva e potencia a adição de riscos associados à sua transmissão, processamento e armazenamento num local de agregação central, ainda que este seja sujeito às medidas de proteção da informação no CNCS consideradas adequadas ao tratamento de matérias classificadas com o grau de segurança Reservado na marca Nacional.* (Universidade de Aveiro, p. 1).

É também indicado pela entidade NOWO/ONI relativamente ao artigo 4.º do projeto de Regulamento que: *Entende-se que esta redação implica que o inventário de ativos deverá abranger ativos que se encontram no âmbito do Regulamento SIRSCE, levando a uma duplicação de elementos nos inventários feitos ao abrigo daquele Regulamento e do DL Regulamentar da Lei de Segurança do Ciberespaço. Consideramos que esta duplicação é indesejável, por duplicar esforços de gestão de inventários e sobrepor âmbitos de atuação operacional. Assim, consideramos que deve ser claramente delimitado o âmbito dos ativos a incluir no inventário regulado por esta instrução técnica, de forma a excluir todos os ativos já abrangidos pelo Regulamento SIRSCE. Por outro lado, a definição de "Ativo" como sendo "todo o sistema de informação e comunicação" e a referência a ativos que suportam "indiretamente, um ou mais serviços" são demasiado vagas e abrangentes. Por razões de eficiência operacional, consideramos que o inventário se deve limitar a ativos que dão suporte direto aos serviços prestados pela empresa e que se encontram abrangidos pela Lei de Segurança do Ciberespaço. Assinala-se, por fim, que a informação detalhada solicitada nos pontos 2 e 3 para os ativos a inventariar inclui elementos (ex: endereços de IP, versões de software, endereços de hardware), que pela sua natureza, são passíveis de alterações frequentes ou constantes, o que torna a gestão do inventário demasiado onerosa para a empresa. Sugere-se que esses elementos sejam eliminados* (NOWO/ONI, p. 2).

É também referido pela EDP relativamente ao mesmo artigo: *é essencial que se defina claramente o que entende por "ativos essenciais". A considera ainda que esta definição de "ativos essenciais" deveria estar ligada à definição de processos de serviços essenciais do operador, para se conseguir balizar o âmbito do inventário (…) a EDP assume, desde logo, que os ativos a que se reporta o Projeto serão apenas os ativos que suportam a prestação dos serviços considerados como essenciais/críticos (…) Acresce que seria conveniente identificar a periodicidade da revisão do inventário, na medida em que, de um ponto de vista prático e operacional, poderá revelar-se impraticável a manutenção do inventário permanentemente atualizado* (EDP, p. 6). É

também indicado pela mesma entidade: *será essencial clarificar o que se entende por "dispositivo físico", devendo precisar-se como devem ser tratados os dispositivos alojados em servidores virtuais ou em cloud (…) será essencial que se identifique claramente o âmbito desta obrigação de comunicação e, em particular, se clarifique que ativos estarão cobertos pela obrigação, atendendo ao carácter genérico e impreciso da expressão "ativos direta ou indiretamente acessíveis publicamente através da Internet".* (EDP, p. 7). É também indicado pela mesma entidade: *Note-se que a informação a comunicar deverá ser restrita, já que uma comunicação detalhada dos ativos ao CNCS acarreta riscos para as organizações, convertendo o CNCS num Single Point of Failure, agregando toda a informação de ativos essenciais. Assim a EDP considera que apenas deveria ser comunicada informação relativa às interfaces da rede técnica que estão expostas à Internet (usadas para acesso remoto), sem prejuízo de, em sede de auditoria/fiscalização, o CNCS poder naturalmente aceder a toda a informação constante do inventário. Acresce que o elenco de informação a comunicar ao CNCS não deverá, no entendimento da EDP, aplicar-se aos dispositivos físicos, a que se reporta o número 2 deste Artigo. Saliente-se que, no caso dos ativos físicos, a informação do IP poderá variar em função do tempo, pelo que a EDP considera que a informação referente a "Endereço IP" se deverá substituir por "Endereço IP/FQDN". No caso de ativos lógicos (aplicações), deve ser especificada uma tabela de informação que não inclua o endereço de IP, tendo em conta que a mesma aplicação poderá ser instalada em máquinas diferentes com IPs diferentes* (EDP, p. 7 e 8).

Devem também ser referidos os comentários da Apritel relativamente ao artigo 4.º: *(…) no caso particular dos prestadores de serviços digitais, e especificamente os que oferecem serviços de computação em nuvem (…) os termos e regras propostos para a elaboração de um inventário de ativos são de muito difícil implementação (…) pelas características dinâmicas associadas à prestação destes serviços digitais, o que leva a que alguns destes elementos sejam alterados com alguma frequência e, em consequência disso, à desatualização da informação partilhada com o CNCS. É exemplo desta realidade a lista de servidores físicos associados aos serviços de computação em nuvem ("cloud"), que pode ter que ser redimensionada para fazer face a necessidades pontuais do serviço. O mesmo acontece com as aplicações, onde é possível recorrer a aumentos do poder computacional por períodos de tempo relativamente curtos, na ordem de horas ou mesmo de minutos (…) no que respeita aos ativos a serem considerados neste processo de inventário, em linha com a definição de ativo proposta no artigo 4.º2, estes devem estar limitados aos sistemas, recursos e elementos físicos e lógicos ligados à prestação dos serviços em causa. A APRITEL entende que estes ativos devem estar ainda limitados aos que são geridos e detidos pelos prestadores, assim como aos que estão associados aos serviços diretamente controlados e desenhados pelos prestadores de serviços digitais. Por fim, devem ser excluídos do âmbito deste inventário os ativos que já constem do inventário que os prestadores de redes e serviços de comunicações eletrónicas já estão obrigados a manter no âmbito do Regulamento de Segurança da ANACOM.* (Apritel, p. 3 e 4).

São ainda realizadas propostas de redação dos n.ºs 1, 3, e 4 do artigo 4.º do projeto de Regulamento pela entidade Câmara Municipal de Portimão, no sentido de efetuar uma correção de redação e uma formulação mais direta do mesmo artigo.

Posição do CNCS

Relativamente aos comentários efetuados deve ser referido que foi entendido pertinente considerando o teor dos mesmos, nomeadamente quanto à solicitação de clarificação da definição de ativos, quanto à consideração do tratamento a dispensar a ativos das entidades indiretamente acessíveis através da Internet e ainda quanto ao tratamento a dispensar a ativos relativos a serviços de computação em nuvem utilizados ou geridos pelas entidades, reformular o artigo 4.º acolhendo as sugestões efetuadas nos seguintes termos. Assim, entende-se que o n.º 1 do artigo 4.º deverá passar a ter a seguinte redação:

1 — Para os efeitos do disposto na presente instrução, entende-se por «Ativo» todo o sistema de informação e comunicação, os equipamentos e os demais recursos físicos e lógicos considerados essenciais, geridos ou detidos pela entidade, que suportam, direta ou indiretamente, um ou mais serviços.

A redação aprovada para o n.º 1 do artigo 4.º do projeto de Regulamento integra agora a referência a recursos geridos ou detidos pela entidade, servindo assim para o esclarecimento de questões relativas á própria definição de ativo e respetiva utilização pelas entidades, assim como quanto à inclusão nesta identificação de ativos de serviços de *Infrastructure-as-a-Service (IaaS)* e *Platform-as-a-Service (PaaS)* utilizados pela entidade.

A redação do artigo 4.º mantém a referência à informação complementar relativa aos equipamentos sobre identificação do endereço de hardware, considerando-se que esta informação tal como consta das medidas previstas no Quadro Nacional de Referência para a Cibersegurança é essencial na gestão de ativos a realizar por qualquer entidade.

Deve também ser referido que foi considerado necessário eliminar a referência às medidas ID.GA Quadro Nacional de Cibersegurança, de acordo com o entendimento de que uma disposição regulamentar não deve remeter para referência técnica não normativa, mantendo-se, no entanto, o respetivo teor na íntegra para aplicação pelas entidades.

Também relativamente ao artigo 4.º foi entendido, atendendo aos comentários efetuados, reformular o respetivo n.º 3, tendo sido aprovada a seguinte redação:

3 — Para efeitos do n.º 3 do artigo 6.º do Decreto-Lei n.º 65/2021, de 30 de julho de 2021, as entidades devem comunicar ao CNCS, com base no inventário de ativos a que se refere o n.º 1 do artigo 6.º do referido normativo, para todos os ativos diretamente acessíveis publicamente através da Internet, uma lista com a seguinte informação:

i) Serviço suportado;
ii) Nome do equipamento/Nome do software;
iii) Modelo/Versão;
iv) Endereço IP (se aplicável);
v) Fully Qualified Domain Names (FQDNs) (se aplicável);
v) Fabricante.

Com a presente redação deixam assim de ser considerados os ativos não diretamente acessíveis através da Internet, ou indiretamente acessíveis através da Internet, para integração de lista de ativos a enviar ao CNCS, sendo assim apenas considerados os ativos diretamente acessíveis através da Internet. Foi ainda incluída como informação a constar desta lista, e também de acordo com sugestão acolhida, informação sobre os

Fully Qualified Domain Names (FQDNs) se aplicável, no mesmo sentido foi entendido poder não ser conhecida a informação sobre os endereços de IP, passando assim esta informação a ser enviada apenas se aplicável pela entidade. Foi de acordo com esta alteração, alterado também o Anexo III do projeto de Regulamento.

Deve ainda ser esclarecido relativamente a comentário efetuado pela EDP quanto à periodicidade da revisão do inventário de ativos, que a referida periodicidade consta já da alínea b) do n.º 3 do artigo 6.º do Decreto-Lei n.º 65/2021, de 30 de julho, de acordo com o qual a lista de ativos deve ser remetida com uma periodicidade anual ao CNCS.

Deve ainda ser referido que a recolha e tratamento de informação relativa à lista de ativos a remeter ao CNCS pelas entidades, se entende como necessária para ações desta entidade para prevenção e resposta a incidentes, de acordo com as respetivas competências tal como estabelecidas nos n.ºs 2 do artigo 7.º da Lei n.º 46/2018, de 13 de agosto, e no artigo 9.º do mesmo normativo.

Deve também ser referido que o setor das comunicações eletrónicas não se encontra no âmbito de aplicação da Lei n.º 46/2018, de 13 de agosto e assim do Decreto-Lei n.º 65/2021, de 30 de julho, não podendo assim ser considerada a respetiva legislação no setor das comunicações eletrónicas como lex specialis nos termos do n.º 2 artigo 18.º do Decreto-Lei n.º 65/2021, de 30 de julho, entendendo-se ainda que o respetivo objeto é diverso do objeto normativo referente à cibersegurança.

Refira-se ainda que se entende que o tratamento de informação nos termos indicados no n.º 3 do artigo 1.º do projeto de Regulamento, é o adequado para a salvaguarda da segurança de informação, de acordo com os termos do qual o CNCS mantém e gere a informação recebida, num sistema de informação seguro em conformidade com as disposições respeitantes à segurança de matérias classificadas com o grau de segurança Reservado na marca Nacional, salvo quando necessário grau de segurança superior.

3.5. **Artigo 5.º**

Relativamente ao artigo 5.º foram apresentados comentários no sentido de se sugerir *uma clarificação no sentido de aferir se o relatório deve inclui o relato de eventuais incidentes reportados por entidades que estejam em base consolidada com a casa-mãe, no que respeita aos operadores de serviços essenciais (setor bancário). Esta obrigação já existe no âmbito da Instrução n.º 21/2019 do Banco de Portugal referente ao reporte de Incidentes de Cibersegurança* (Caixa Geral de Depósitos).

Foi também sugerido pela Câmara Municipal de Portimão a disponibilização de *modelo XML, ou um outro qualquer modelo pré formatado de metadados* para envio do relatório anual ao CNCS pelas entidades e uma proposta de redação para o n.º 2 do projeto de Regulamento.

É também referido pela entidade Hospital Distrital da Figueira da Foz, EPE, relativamente ao artigo 5.º do projeto de Regulamento e ao Anexo IV aplicável nos termos do referido artigo: *percebe-se a utilização de standards como referência e, também a criação exacerbada quer do volume de dados quer da importância à centralização dessa mesma informação. É uma descrição demasiado exaustiva, nomeadamente a relativa ao levantamento de riscos. A realização dos relatórios poderia ser disposta numa página, a construir e disponibilizar para o efeito; as informações adicionais, registos de ataques, consequencias e a evolução dos ativos e dos riscos seriam parte das "versões" a existir. Desta forma seria muito mais eficaz a análise e a manutenção da informação: útil para a CNCS e útil para as entidades.*

Posição do CNCS

Relativamente aos comentários realizados pelas entidades relativamente ao artigo 5.º do projeto de Regulamento deve ser referido que a informação a constar do referido relatório é desde logo indicada no n.º 1 do artigo 8.º do Decreto-Lei n.º 65/2021, de 30 de julho, sendo o mesmo aplicado por cada entidade no âmbito do Decreto-Lei n.º 65/2021, de 30 de julho, assim quanto à informação relativa a incidentes ocorridos esta informação reporta-se aos incidentes ocorridos em cada entidade que deverá elaborar e enviar o relatório anual ao CNCS.

Relativamente ao modelo de formulário para envio de informação com o relatório anual ao CNCS, este consta já do Anexo IV a que se refere o artigo 5.º do projeto de regulamento, sendo entendido que o tipo de ficheiro PDF serve o processamento de informação a realizar pelo CNCS.

Relativamente à proposta de redação do n.º 2 do artigo 5 do projeto de Regulamento, apresentada pela Câmara Municipal de Portimão, entende-se que a formulação atual é facilmente percetível para execução e nesse sentido facilitadora e mais clara para aplicação pelas entidades destinatárias deste normativo, mantendo-se assim os termos de redação propostos.

Deve ainda novamente referir-se que a informação a constar do relatório anual consta já do n.º 1 do artigo 8.º do Decreto-Lei n.º 65/2021, de 30 de julho, devendo também referir-se que os elementos constantes do mesmo estão de acordo com a recolha e tratamento de informação a realizar pelo CNCS, entendendo-se esta informação como necessária para a supervisão a realizar por esta entidade no domínio da aplicação de medidas de segurança e para a resposta desta entidade através do CERT.PT a incidentes ocorridos e à prevenção de incidentes, de acordo com as respetivas competências tal como estabelecidas nos n.ºs 2 e 4 do artigo 7.º da Lei n.º 46/2018, de 13 de agosto, e no artigo 9.º do mesmo normativo.

3.6. **Artigo 6.º**

Relativamente ao artigo 6.º do projeto de Regulamento, foi apresentada sugestão pela Caixa Geral de Depósitos no sentido de ser realizada clarificação *sobre a eventual divergência que possa vir a ocorrer entre a designação e caraterização dos incidentes referidos na Lei n.º 46/2018 (Regime Jurídico da segurança do ciberespaço) e os incidentes referidos na Instrução n.º 21/2019 do BdP (Reporte de incidentes de cibersegurança).*

É também realizada uma sugestão de *normalização de tipologias e de métricas para melhoria da análise situacional integrada, no âmbito da gestão de ciberincidentes* pela entidade Necho Tech Law, que se entende ser reconduzida ao artigo 16.º do Decreto-Lei n.º 65/2021, de 30 de julho, referente a Taxonomia de incidentes e de efeitos.

É também realizada sugestão pela entidade EDP que se entende enquadrada no âmbito dos termos do Decreto-Lei n.º 65/2021, de 30 de julho no que concerne à notificação de incidentes. Assim é referido: *O Projeto regulamenta a forma de notificação de incidentes, nos termos e para os efeitos dos artigos 11.º a 16.º do Decreto-Lei n.º 65/2021. Contudo, não são concretizados os critérios para a sua respetiva classificação como tendo impacto relevante ou substancial. A EDP considera que esta concretização é essencial, sob pena de comprometer uma aplicação coerente e harmonizada entre as diferentes entidades abrangidas, comprometendo o objetivo primordial do regime de reforço da resiliência.*

Também em referência ao enquadramento normativo do Decreto-Lei n.º 65/2021, de 30 de julho, é referido pela entidade NOWO/ONI: (…) *uma vez que o sector das comunicações eletrónicas já emite notificações de incidentes à ANACOM através de formatos e procedimentos definidos no Regulamento SIRSCE, tendo os operadores de comunicações eletrónicas desenvolvidos sistemas de notificação para esse fim, era nossa expectativa poder continuar a utilizar esses formatos, procedimentos e sistemas de notificação para as notificações ao CNCS. Aliás, na consulta pública sobre o projeto de decreto-lei que deu origem ao Decreto-Lei nº 65/2021, foi essa a posição que defendemos, a qual teve acolhimento através da disposição acima citada desse Decreto-Lei. Face ao exposto, solicita-se que no Projecto de Regulamento relativo à instrução técnica seja clarificado que: a) As entidades devem seguir o formato e procedimento de notificação de incidentes definido nos normativos complementares setoriais aplicáveis b) Na ausência de tais normativos, devem as entidades notificar o CNCS através do modelo de reporte existente para esse efeito no seu sítio na Internet* (NOWO/ONI, p. 3).

É também referido pela entidade Apritel quanto ao artigo 6.º do projeto de Regulamento: *A respeito do âmbito de notificação a ser efetuado pelos prestadores de serviços digitais, a APRITEL entende que este deve estar limitado aos serviços que são diretamente controlados e geridos por estes prestadores, sobre os quais detêm acesso a informação necessária para avaliar o impacto de um incidente. Neste sentido, devem estar excluídos todos os serviços que impliquem a intervenção de outras entidades na prestação das ofertas aos utilizadores finais. Por exemplo, os incidentes que afetem o acesso a serviços que sejam objeto de revenda não devem ser notificados pelos prestadores que efetuam esta revenda, mas antes pelas entidades responsáveis pela gestão destas ofertas (…) a APRITEL sugere a criação de uma API4 que permita*

garantir a automatização deste processo de notificação (…) a APRITEL não pode deixar de demonstrar a sua preocupação quanto ao facto de o acesso ao formulário poder ser feito sem o recurso a qualquer processo de autentificação (…) a APRITEL considera essencial que sejam desenvolvidos mecanismos de autentificação para o envio destas notificações (…) em caso de falha destes meios de notificação, sugere-se que o CNCS disponibilize um contacto telefónico para este fim, o qual, por razões de confidencialidade, deverá apenas ser comunicado aos responsáveis de segurança das empresas (Apritel, p. 4, 5, 6).

Decorre ainda dos comentários remetidos pela entidade ANA – Aeroportos de Portugal o entendimento veiculado por esta entidade como sendo a mesma a dever realizar a notificação de incidentes ao CNCS nos termos previstos no Decreto-Lei n.º 65/2021, de 30 de julho, de acordo com os termos propostos no artigo 6.º do projeto de Regulamento, relativamente aos incidentes ocorridos em qualquer das infraestruturas aeroportuárias sob a respetiva gestão concessionária.

Posição do CNCS

Relativamente às sugestões apresentadas foi considerado pertinente acolher a sugestão da Apritel no sentido de utilização de API a disponibilizar pelo CNCS, tendo assim sido aprovada a seguinte redação do n.º 1 do artigo 6.º do projeto de Regulamento:

1 — O envio das notificações de incidentes e de informação adicional, de acordo com os termos dos artigos 11.º a 16.º do Decreto -Lei n.º 65/2021, de 30 de julho de 2021, com produção de efeitos prevista no n.º 2 do artigo 23.º, deve ser realizado através do sítio na Internet do Centro Nacional de Cibersegurança (https://www.cncs.gov.pt) na funcionalidade «Notificação de Incidentes», mediante o preenchimento do modelo de reporte estabelecido para o efeito, ou via API (application programming interface) disponibilizada pelo CNCS para o efeito.

Ainda relativamente aos comentários desta entidade deve esclarecer-se que as alíneas b) e c) do n.º 2 do artigo 6.º do projeto de Regulamento indicam já contato telefónico para utilização pelas entidades, para realização de notificação de incidentes, estando um dos referidos contactos telefónicos em disponibilidade contínua 24 horas por dia, sete dias por semana.

Relativamente aos demais comentários, nomeadamente para definição dos limites para além dos quais um incidente é considerado relevante ou substancial, e normalização de tipologias, deve ser primariamente referido que a presente consulta pública é referente ao conteúdo do projeto de Regulamento que configura instrução técnica constante do Aviso 21606/2021, assim não se refere ao conteúdo e termos do Decreto-Lei n.º 65/2021, de 30 de julho, o qual foi objeto de consulta pública anterior. Deve ainda referir-se que a previsão dos artigos 11.º a 16.º do Decreto-Lei n.º 65/2021 é necessariamente transversal e aplicável a todos os setores no âmbito de aplicação da Lei n.º 46/2018, de 13 de agosto e do Decreto-Lei n.º 65/2021, de 30 de julho. Considera-se, assim, que a regulamentação a aprovar para efeito da definição dos limites de notificação de incidentes para além dos quais um incidente é considerado relevante em cada setor fica no âmbito de aplicação do artigo 18 (1, 2) do Decreto-Lei n.º 65/2021, de 13 de agosto, quer seja através de Instrução específica para o efeito, quer seja através da apreciação

de equivalência de normativos setoriais existentes que possam ser objeto de Instrução a emitir pelo CNCS que remeta para a aplicação dos mesmos.

Ainda relativamente à definição do limite para além do qual um incidente é considerado como substancial, deve referir-se nos termos do n.º 1 do artigo 19.º da Lei n.º 46/2018, de 13 de agosto, que relativamente aos prestadores de serviços digitais, o limite de um incidente considerado substancial se encontra definido no Regulamento de Execução (UE) 2018/151, da Comissão, de 30 de janeiro de 2018, em matéria de requisitos de segurança e de notificação de incidentes, o qual se aplica diretamente a estas entidades, veja-se com esta referência o disposto no n. 4 do artigo 3.º do Decreto-Lei n.º 65/2021, de 30 de julho.

Deve também ser considerado que o setor das comunicações eletrónicas não se encontra no âmbito de aplicação da Lei n.º 46/2018, de 13 de agosto e assim do Decreto-Lei n.º 65/2021, de 30 de julho, não podendo assim ser considerada a respetiva legislação no setor das comunicações eletrónicas como lex specialis nos termos do n.º 2 artigo 18.º do Decreto-Lei n.º 65/2021, de 30 de julho, entendendo-se ainda que o respetivo objeto é diverso do objeto normativo referente à cibersegurança.

Deve ainda ser referido que as entidades no âmbito de aplicação da Lei n.º 46/2018, de 13 de agosto e do Decreto-Lei n.º 65/2021, de 30 de julho são identificadas nos termos da tipologia prevista no artigo 2.º da referida Lei, para o qual remete o n.º 1 do artigo 2.º do Decreto-Lei n.º 65/2021, de 30 de julho, sendo assim as obrigações decorrentes do Decreto-Lei n.º 65/2021, de 30 de julho aplicadas de acordo com esta mesma tipologia. De acordo com a identificação prevista na Lei n.º 46/2018, de 13 de agosto, as entidades consideradas como operadores de serviços essenciais são definidas nos termos das alíneas g) e t) do artigo 3.º do mesmo normativo como uma entidade pública ou privada que presta um serviço essencial para a manutenção de atividades societais ou económicas cruciais, que dependa de redes e de sistemas de informação e em relação ao qual a ocorrência de um incidente possa ter efeitos perturbadores relevantes na prestação desse serviço.

Nestes termos, os operadores de serviços essenciais foram identificados com a colaboração das entidades reguladoras e com poderes de supervisão nos diferentes setores e subsetores de acordo com critérios aplicados setorialmente, tendo sido identificadas e formalmente notificadas as entidades que realizam serviços essenciais de acordo com a tipologia definida no anexo à Lei n.º 46/2018, de 13 de agosto. Com este enquadramento aplica-se o n.º 5 do artigo 3.º do Decreto-Lei n.º 65/2021, de 30 de julho, nos termos do qual as entidades referidas no n.º 1 do artigo 2.º deste normativo podem estabelecer formas de colaboração com vista ao cumprimento das obrigações em matéria de requisitos de segurança e de notificação de incidentes previstos no Regime Jurídico da Segurança do Ciberespaço, e no Decreto-Lei n.º 65/2021, de 30 de julho, numa lógica de partilha de recursos, desde que seja assegurada a efetiva operacionalização das mesmas em cada entidade.

4. Conclusão

Tendo em consideração as pronúncias recebidas e o seu entendimento sobre as mesmas, o CNCS realizou as alterações ao projeto de Regulamento assinaladas, tendo ainda sido realizada a correspondente atualização das referências dos Anexos ao projeto de Regulamento. A redação agora aprovada do projeto de Regulamento tem como objetivo uma aplicação clarificada e facilitada pelas entidades destinatárias deste normativo, e a implementação transversal aos diferentes setores sob supervisão do Centro Nacional de Cibersegurança do Decreto-Lei n.º 65/2021, de 30 de julho, sem prejuízo da futura aprovação de Instruções técnicas com âmbito de aplicação setorial, nomeadamente, nos termos dos n.ºs 1 e 2 do artigo 18.º do Decreto-Lei n.º 65/2021, de 30 de julho.