COMENTÁRIOS DA EDP - ENERGIAS DE PORTUGAL, S.A.

À CONSULTA PÚBLICA

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

I. Introdução

Foi colocado, em consulta pública, o projeto de regulamento que configura instrução técnica do Centro Nacional de Cibersegurança ("**CNCS**") relativa à comunicação e informação referentes a pontos de contacto permanente, responsável de segurança, inventário de ativos, relatório anual e notificação de incidentes (doravante "**Projeto**").

O Projeto vem regulamentar algumas obrigações previstas no **Decreto -Lei n.º 65/2021**, de 30 de julho, decorrentes da **Lei n.º 46/2018**, de 13 de agosto.

Em particular, o Projeto regulamenta as seguintes disposições do Decreto-Lei n.º 65/2021:

(i) n.ºs 3, 4 e 5 do artigo 4.º, referente à indicação de **ponto de contacto permanente**;

(ii) n.ºs 2, 3 e 4 do artigo 5.º referente à indicação do **responsável de segurança**;

(iii) n.ºs 1, 2 e 3 do artigo 6.º referentes à informação que, para cada ativo, deve constar do **inventário de ativos** e à comunicação da lista de ativos;

(iv) n.ºs 1, 2, 3 e 4 do artigo 8.º relativo à informação que deve constar do **relatório anual** e à comunicação do relatório anual;

(v) n.ºs do artigo 12.º, n.º 1 do artigo 13.º, n.º 1 do artigo 14.º, n.º 1 do artigo 15.º e n.º 2 do artigo 17.º referentes ao envio das **notificações de incidentes** e de informação adicional.

Analisado o Projeto, a EDP – Energias de Portugal, S.A. bem como a EDP - Gestão da Produção de Energia, S.A. (em conjunto, "**EDP**") gostaria de transmitir, desde logo, que a regulamentação do regime jurídico da segurança do ciberespaço constitui um importante desenvolvimento com um potencial de aumento do nível de segurança dos dados e da informação.

Contudo, a EDP considera que existem aspetos, no Projeto, que requerem uma análise e ponderação cuidada.

Assim, a EDP toma a iniciativa de submeter o seu contributo para esta Consulta Pública, como forma de sugerir determinadas alterações e esclarecimentos ao clausulado proposto.

II. Enquadramento e Comentários gerais

O setor europeu da energia atravessa uma importante e disruptiva mudança rumo a uma economia descarbonizada que garanta, simultaneamente, a segurança do aprovisionamento e a

competitividade. No âmbito desta transição energética e da descentralização da produção de energia a partir de fontes renováveis, a rede elétrica da Europa está a transformar-se numa "rede inteligente", o que acarreta novos riscos desde logo relacionados com cibersegurança.

É neste contexto que o pacote legislativo "Energia Limpa para todos os Europeus" reconhece a importância da cibersegurança para o setor da eletricidade.

O tema da cibersegurança e proteção de redes e sistemas tem sido, consistentemente, uma preocupação e uma prioridade para a EDP, tendo vindo a efetuar importantes investimentos e adaptações nesta sede. Tratando-se de uma preocupação estrutural, a EDP sempre se tem disponibilizado para, junto das entidades e autoridades competentes, participar na discussão e construção de um quadro de resiliência. Assim, e como nota inicial, a EDP congratula a iniciativa e o foco do legislador nos temas de cibersegurança, considerando que o Projeto constitui uma importante, e muito aguardada, peça na regulação da cibersegurança.

Com esta resposta, a EDP espera contribuir positiva e construtivamente para o desenvolvimento de um ambiente de resiliência e de confiança, partilhando a sua visão e experiência bem como desafios sentidos na implementação das obrigações densificadas pelo Projeto.

De facto, a operacionalização de algumas obrigações e procedimentos constantes do Projeto em apreço implicam um esforço e dedicação considerável, pelo que a EDP espera que os seus contributos sejam considerados pelo CNCS.

Deste modo, a EDP gostaria, desde já, de partilhar os seguintes comentários de natureza geral:

1. Em primeiro lugar, nota-se que as obrigações que o Projeto vem regulamentar, e que decorrem do Decreto-Lei n.º 65/2021, já se encontram, à data, em vigor, não tendo sido prevista qualquer prorrogação do respetivo prazo de implementação.

Ora, o cumprimento das referidas obrigações reveste-se de extrema dificuldade para as organizações, quando a forma específica da sua implementação ainda se encontra em discussão.

2. Acresce que o Projeto não versa sobre o Plano de Segurança, obrigação que nos termos do Decreto-Lei n.º 65/2021 se encontra também em vigor, o que inevitavelmente compromete a sua cabal e eficiente implementação.

Como tal, a EDP considera que o CNCS deveria emitir, com a maior brevidade, uma instrução técnica relativa à obrigação de elaboração do Plano de Segurança que clarifique, desde logo, os seguintes aspetos: (i) o formato e nível de exigência/requisitos do plano e (ii) nível de detalhe exigido na "descrição de todas as medidas adotadas".

3. Note-se ainda que o Projeto, à semelhança do que sucede com o Decreto-Lei n.º 65/2021, utiliza alguns conceitos vagos e indeterminados, o que poderá levar a interpretações distintas pelas entidades cobertas, comprometendo o objetivo de construção de um ambiente que garanta a resiliência das entidades cobertas.

Assim, seria importante que o legislador concretizasse os conceitos utilizados, de forma a permitir uma harmonização e aplicação coerente entre os destinatários das obrigações.

4. A EDP reitera o que já teve oportunidade de partilhar aquando da resposta à consulta pública no âmbito do Decreto-Lei n.º 65/2021, relativamente à oportunidade do Projeto. A este respeito, a EDP considera que o Projeto deveria, desde já, preparar as organizações para aquele que será o futuro quadro legal em matéria de cibersegurança, desde logo decorrente das propostas de Diretiva SRI revista ou SRI 2[1] e a nova diretiva relativa à resiliência das entidades críticas[2].

Assim, e não obstante se tratarem ainda de propostas de Diretivas, a EDP considera que a densificação das obrigações por via de instruções técnicas do CNCS deverá, tanto quanto possível, ser alinhado com as propostas apresentadas a nível Europeu.

5. Por fim, na medida em que o Projeto versa sobre matérias que são reguladas igualmente através de outros instrumentos, será importante que, na emissão de instruções técnicas pelo CNCS, sejam tidas em consideração as obrigações já existentes em diversos diplomas – como

[1] Disponível em https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union
[2] Disponível em https://ec.europa.eu/home-affairs/sites/default/files/pdf/15122020_proposal_directive_resilience_critical_entities_com-2020-829_en.pdf

é o caso, desde logo, do Regulamento Geral sobre a Proteção de Dados[3] ("**RGPD**") e do Decreto-Lei n.º 62/2011 de 9 de maio[4] ("**Regime das Infraestruturas Críticas**").

A este respeito, note-se que o Regime das Infraestruturas Críticas é particularmente central para a atividade da EDP - Gestão da Produção de Energia, S.A., que se dedica à exploração de ativos de produção hídrica e térmica, que fornecem apoio e resiliência ao sistema elétrico nacional na transição para uma energia mais distribuída e limpa. Ao contrário da geração distribuída, as operações críticas destes ativos, alguns dos quais se enquadram na classificação de infraestruturas críticas no âmbito do Decreto-Lei n.º 62/2011, baseiam-se em redes e sistemas de informação que são tipicamente isolados e protegidos das redes públicas, com a conectividade restrita a certas funções específicas.

III. Comentários Específicos

Apresentados os comentários iniciais e gerais, analisam-se, de seguida, as disposições que a EDP considera deverem ser densificadas, ponderadas e/ou revistas.

TÓPICO	COMENTÁRIOS EDP
Ponto de contacto permanente (Artigo 2.º)	Prevê-se que as entidades cobertas pelo regime comuniquem, ao CNCS, o ponto de contacto permanente, devendo disponibilizar um conjunto de informação prevista no número 2 do Artigo 2.º, de entre as quais se destaca o número de telefone fixo. 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.
Responsáveis de segurança (Artigo 3.º)	Prevê-se que as entidades cobertas comuniquem, ao CNCS, o responsável de segurança, devendo disponibilizar um conjunto de informação prevista no número 2 do Artigo 3.º, de entre as quais se destaca o número de telefone fixo.

[3] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE.

[4] Estabelece os procedimentos de identificação e de proteção das infraestruturas essenciais para a saúde, a segurança e o bem-estar económico e social da sociedade nos sectores da energia e transportes e transpõe a Diretiva n.º 2008/114/CE, do Conselho, de 8 de dezembro.

	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.
Inventário de ativos (Artigo 4.º n.º 1)	O Decreto-Lei n.º 65/2021 prevê, no seu artigo 6.º, a obrigação das entidades abrangidas elaborarem e manterem atualizado "**um inventário de todos os ativos essenciais para a prestação dos respetivos serviços**." Por sua vez, o Projeto prevê, no seu artigo 4.º n.º 1, que se entende por "**Ativo**" todo o sistema de informação e comunicação, os equipamentos e os demais recursos físicos e lógicos considerandos essenciais, que suportam, direta ou indiretamente, um ou mais serviços. É essencial que se defina claramente o que entende por "ativos essenciais". A EDP considera ainda que esta a definição de "ativos essenciais" deveria também estar ligada à definição de processos de serviços essenciais do operador, para se conseguir balizar o âmbito do inventário. A este respeito, e considerando o âmbito de aplicação da Lei n.º 46/2018, a EDP assume que os ativos a que se reporta o Projeto serão apenas os **ativos que suportam a prestação dos serviços considerados como essenciais/críticos** e, no caso particular da EDP Gestão de Produção de Energia Elétrica S.A., relativamente às infraestruturas críticas que determinam a sua classificação ao abrigo do Regime das Infraestruturas Críticas. 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.
Inventário de ativos (Artigo 4.º n.º 2)	No número 2 do Artigo 4.º, o Projeto refere que a informação a constar do inventário de ativos deve ser baseada nas medidas técnicas ID.GA -1 — Os dispositivos físicos, redes e sistemas de informação existentes na organização devem ser inventariados e ID.GA-2— As aplicações e plataformas de software que suportam os processos dos serviços críticos devem ser inventariadas. A este respeito, e considerando o âmbito de aplicação da Lei n.º 46/2018, a EDP assume, desde logo, que **os ativos a inventariar nos termos deste número**

	serão apenas os ativos que suportam a prestação dos serviços considerados como essenciais/críticos e, no caso particular da EDP Gestão de Produção de Energia Elétrica S.A., relativamente às infraestruturas críticas que determinam a sua classificação ao abrigo do Regime das Infraestruturas Críticas. Quanto à informação a constar do inventário, e no que respeita os **dispositivos físicos** e sistemas a inventariar de acordo com a medida técnica ID.GA – 1, será essencial clarificar o que se entende por "dispositivo físico", devendo precisar-se como devem ser tratados os sistemas alojados em servidores virtuais ou em *cloud*.
Inventário de ativos (Artigo 4.º n.º 3)	Estabelece-se que, com base no inventário elaborado, as entidades abrangidas comuniquem ao CNCS, para todos os ativos direta ou indiretamente acessíveis publicamente através da Internet, uma lista de ativos com a seguinte informação: (a) serviço suportado, (b) nome do equipamento/software, (c) modelo/versão, (d) endereço IP, (e) fabricante. Como nota geral, a EDP destaca que, atendendo à sensibilidade da informação, 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", tendo igualmente em conta que, como indicado acima, no caso da EDP Gestão de Produção de Energia Elétrica S.A. os ativos que suportam operações críticas são tipicamente redes isoladas. 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 ainda que, no caso dos ativos físicos, a informação do IP poderá variar em função do tempo, pelo que a EDP considera que a informação "Endereço IP" se deveria substituir por "Endereço IP/FQDN". No caso de ativos lógicos (aplicações), deve ser especificada uma tabela de informação que não inclua o endereço IP, tendo em conta que a mesma aplicação pode ser instalada em máquinas diferentes com IPs diferentes.
Notificação de incidentes (Artigo 6.º)	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.

IV. Conclusões

Atento ao acima exposto, a EDP gostaria de salientar, em jeito de conclusão, os seguintes aspetos:

1. Em primeiro lugar, a EDP congratula a iniciativa e o foco do legislador na regulação dos temas de cibersegurança, considerando que o Projeto constitui uma importante peça nesta sede.
2. A EDP considera, contudo, que a oportunidade do Projeto é comprometida pelos prazos de entrada em vigor e implementação das obrigações que o mesmo vem regular, já que, à data, já as organizações têm de ter implementado um conjunto de obrigações, cujo formato e aspetos prático de aplicação se encontram em consulta pública.
3. Acresce que seria importante que o Projeto versasse igualmente sobre a obrigação de elaboração de um plano de segurança – obrigação que também já se encontra em vigor – e em relação à qual a EDP considera existirem ainda inúmeras indefinições.

4. Salienta-se ainda que existem algumas disposições do Projeto que carecem de clarificação e densificação, sob pena de prejudicar a sua aplicação harmonizada, uniforme e eficaz por parte das organizações. Desde logo, no que respeita à obrigação de inventariação dos ativos e respetiva comunicação ao CNCS.

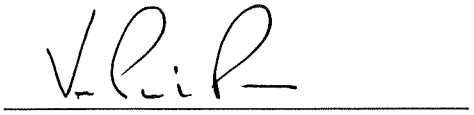
5. Acresce que, atendendo às especificidades dos diversos sectores cobertos, é essencial assegurar que o Projeto será acompanhado por um conjunto de disposições e orientações setoriais, devendo-se promover um alinhamento com os reguladores setoriais nesta matéria. Este aspeto já decorre do preâmbulo do Decreto-Lei n.º 65/2021 que reforça a necessidade de articulação, entre o CNCS e as entidades reguladoras e de supervisão setoriais, devendo assim ser levada a cabo uma avaliação de equivalência entre os requisitos previstos nos vários diplomas setoriais e os previstos no citado Decreto-Lei.

A EDP espera que os seus comentários contribuam para a revisão e reavaliação de alguns aspetos do projeto, construindo-se assim um quadro regulatório que assegure um alinhamento jurídico e proporcione a adoção das melhores práticas em matéria de cibersegurança.

A EDP desde já se disponibiliza para, conjuntamente com o CNCS e/ou outras entidades envolvidas – desde logo, o regulador setorial -, trabalhar no desenvolvimento de mecanismos, metodologias e referenciais de segurança que permitam, às organizações, levar a cabo as avaliações de risco e a implementação das medidas adequadas para a proteção dos dados, da informação e dos seus sistemas.

Lisboa, 27 de dezembro de 2021

Pela EDP - Energias de Portugal, S.A.,



(Vera de Morais Pinto Pereira Carneiro)

(Rui Manuel Rodrigues Lopes Teixeira)