RELATÓRIO

Procedimento Regulamentar para a aprovação de Regulamento de execução do Regime Jurídico da Cibersegurança, aprovado pelo Decreto-Lei n.º 125/2025, de 4 de dezembro – Consulta Pública, nos termos do artigo 101.º do Código do Procedimento Administrativo.

ÍNDICE

I- Enquadramento

Por despacho do Coordenador do Centro Nacional de Cibersegurança (CNCS), de 27 de fevereiro de 2026, e no uso de competência delegada, por força do da alínea a) do n.º 1 do Despacho n.º 8875/2025, de 17 de julho, do Diretor-Geral do Gabinete Nacional de Segurança, publicado no Diário da República n.º 145, 2.ª Série, de 30 de julho, foi aprovado o projeto de regulamento do Regime Jurídico de Cibersegurança, aprovado pelo Decreto-Lei n.º 125/2025, de 4 de dezembro.

O mencionado projeto de Regulamento esteve em consulta pública pelo período de 30 dias úteis, nos termos do n.º 2 do artigo 101.º do Código do Procedimento Administrativo.

A consulta pública decorreu de 10/03/2026 a 22/04/2026, tendo o CNCS recebido respostas e contributos de 56 entidades e particulares. Por questões de economia de espaço as entidades e particulares encontram-se elencados abaixo.

Sem prejuízo, será garantida a preservação de qualquer informação reservada ou de segredo comercial ou outros que tenha sido partilhada.

O presente Relatório contém referência a todas as respostas recebidas e uma apreciação global que reflete o entendimento do CNCS sobre as mesmas. Os contributos serão disponibilizados em tabela para melhor compreensão.

O Coordenador do Centro Nacional de Cibersegurança

Assinado por: **José Lino Alves dos Santos**
Num. de Identificação: 09880194
Data: 2026.06.22 11:28:54 +0100

_____

Lino Santos

II- Apreciação dos contributos

Contributos	Resultado da apreciação do CNCS	
COMPLEAR		
Contributos e comentários enviados relativamente ao Decreto-Lei nº. 125/2025	Não acolhido	O contributo não respeita, na sua maioria, o objeto da consulta pública e, quando o faz, propõe medidas de segurança física já existentes (vd. PR.GA-6 e DE.MC-2) no Projeto de Regulamento, bem como instruções que estão fora do âmbito do Regulamento, nomeadamente as obrigações do responsável de cibersegurança.
Aquino consultoria		
Transparência da Matriz de risco	Não acolhido	A Matriz não está em consulta pública.
Regulamento deveria prever, de forma mais clara como são aplicados os critérios que conduzem à classificação das entidades	Não acolhido	A Matriz densifica suficientemente os critérios de classificação das entidades.
MEO		
Quadro Nacional de Referência para a Cibersegurança- Sugiro que sejam adicionados ao documento a indicação de data, versão e controlo de versão. O documento atual não deixa claro quando foi produzido e a versão do mesmo, gerando dúvidas para os leitores.	Não acolhido	O Quadro Nacional de Referência para a Cibersegurança (QNRCS) não é objeto de consulta pública, sendo que o QNRCS será publicado como Anexo ao Regulamento, sendo essa a data e a versão do mesmo.
Garantia da proteção da informação da lista de ativos	Parcialmente acolhido	O Projeto de Regulamento foi alterado para referir a plataforma onde é submetida a lista de ativos.
Requisitos mínimos a constar no inventário de ativos publicamente acessíveis, garantindo que o CNCS recebe dados úteis para análise de risco nacional e não apenas uma listagem técnica de endpoints.	Parcialmente acolhido.	O Projeto de Regulamento dispõe, no artigo 32º, sobre o que deve constar da lista de ativos publicamente acessíveis, sendo que parte dos elementos do contributo poderão ser formalizados em sede de instrução técnica.

SIA		
Enriquecer a definição de computação em nuvem nas definições do artigo 3.º do Regulamento do Regime Jurídico de Cibersegurança, e caso não seja objetivo abranger a totalidade dos SaaS, clarificar as fronteiras.	Não acolhido	A integração dos SaaS no âmbito subjetivo do Decreto-Lei nº 125/2025 resulta dos critérios já suficientemente densificados e abrangentes no próprio Decreto-Lei.
Detalhar num anexo ao Regulamento do Regime Jurídico da Cibersegurança as atividades económicas abrangidas.	Não acolhido	O legislador optou por não reduzir os setores críticos de atividade previstos no Decreto-Lei nº 125/2025 à identificação por CAE.
Sendo o Anexo ao Decreto-Lei n.º 22/2025 muito parecido com o anexo ao Decreto-Lei n.º 125/2025, devem-se clarificar as entidades que ficam abrangidas pelo Decreto-Lei n.º 125/2025, por força deste alargamento previsto no n. 5.º do artigo 3.º do Decreto-Lei n.º 125/2025 (ex: Transportes públicos: serviços públicos de transporte de passageiros por caminho de ferro e outros sistemas guiados, bem como por estrada (operadores de serviços públicos)).	Não acolhido	O Decreto-Lei nº 22/2025 e o Decreto-Lei nº 125/2025 têm âmbitos de aplicação distintos. Não obstante, a relação entre ambos é expressamente regulada pelo disposto na alínea e) do nº1 do artigo 6º do Decreto-Lei nº 125/2025.
Instituto Português da Acreditação e Certificação		
Definição do organismo competente para a acreditação	Não acolhido	Não é um contributo para efeitos de consulta pública. Não obstante, é uma questão resolvida pela alínea e) do nº2 do artigo 20.º do Decreto-Lei nº 125/2025.
JPB-Especialista de Sistemas e Tecnologias da Informação		
Institucionalização do CISO (Chief Information Security Officer)	Não acolhido	Matéria respeitante à autonomia dos Municípios.
Câmara Municipal de Portimão		
Comunicação à autoridade de cibersegurança	Acolhido	Projeto de Regulamento adaptado para clarificar o prazo de entrega para as

competente da lista de ativos		entidades importantes e públicas relevantes.
Densificação da alínea d) do nº1 do artigo 6º do RJC	Não acolhido	Os critérios dispostos na alínea d) do nº1 do artigo 6º do Decreto-Lei n.º 125/2025 serão devidamente densificados aquando da qualificação das entidades, nos termos do disposto no nº 4 do artigo 8º do Decreto-Lei n.º 125/2025.
Câmara Municipal Cabeceiras de Basto		
Referencial de competências para funções de Responsável de Cibersegurança e Ponto de Contacto	Considerado.	O CNCS emitirá oportunamente orientações técnicas quanto a esta matéria.
Determinação de uma compensação pela disponibilidade contínua de 24 horas por dia e de 7 dias por semana	Não acolhido	Matéria de reserva legislativa.
Falta de clareza sobre qual o tipo de meio de contacto principal e qual o alternativo.	Não acolhido	Os tipos de meio de contacto principal e alternativo estão devidamente esclarecidos e listados no nº3 do artigo 15.º do Projeto de Regulamento.
Criação de uma equipa municipal, dedicada única e exclusivamente à cibersegurança.	Não acolhido	Matéria de autonomia dos municípios.
Obrigatoriedade da criação de um Gabinete para gestão de crises (*disaster recovery*), de forma a garantir a continuidade do negócio e a reposição dos sistemas em casos de incidentes.	Não acolhido	O Regulamento define as medidas mínimas de cibersegurança obrigatórias aplicáveis de forma abrangente, transversal e pretendendo abarcar o maior número de situações. A verificação da aplicação das medidas tem em conta o princípio da proporcionalidade. As entidades públicas que sejam qualificadas como essenciais ou importantes deverão cumprir com as medidas do Anexo III, que inclui requisitos de continuidade de negócio.
Definição de equipa municipal, dedicada exclusivamente à cibersegurança	Não acolhido	A definição de uma equipa municipal dedicada exclusivamente à cibersegurança está fora do âmbito do Regulamento.
CG-Especialista em Resiliência Digital e Governação da Segurança da Informação		

Propostas para medidas de política publica	Não acolhido	Os contributos da entidade não dizem respeito ao âmbito do Regulamento.
Câmara Municipal de Sintra		
Identificação e acesso à plataforma eletrónica	Parcialmente acolhido	Redação do artigo 6.º clarificada.
Alteração da nomenclatura Responsável de Segurança	Acolhido	Redação do artigo 14.º corrigida.
Controlo e rastreabilidade de acessos na plataforma	Acolhido	Redação do artigo 5.º atualizada.
Extração ou exportação das notificações em formato de ficheiro que permita o respetivo tratamento interno	Acolhido	Redação do artigo 22º clarificada.
Clarificar a aplicação das medidas dos artigos 25º, 26º, 29º, 30º e 31º às Entidades Públicas Relevantes	Parcialmente acolhido	Não compete ao Regulamento clarificar a aplicação das medidas às entidades públicas relevantes uma vez que tal disposição decorre do Decreto-Lei n.º 125/2025. O nº1 do artigo 24º do Regulamento foi alterada para esclarecer a questão da aplicação do Quadro Nacional de Referência de Cibersegurança (QNRCS).
Certificação voluntária – exigência explícita do âmbito das certificações apresentadas	Parcialmente acolhido	Redação do artigo 27º alterada.
Carácter voluntário ou obrigatório da certificação-Ambiguidade entre artigo 27º do Regulamento e artigo 34º do RJC	Parcialmente acolhido	Redação do artigo 27º e do artigo 30º do Regulamento alterada.
Quadro Nacional de Referência para Cibersegurança-Definições e Referências a Frameworks	Considerado	O Quadro Nacional de Referência de Cibersegurança (QNRCS) não é objeto de consulta pública, porém, os lapsos foram corrigidos.
Matriz de Risco-Preenchimento da Matriz de Risco, Análise dos valores das fórmulas e disponibilização de mais informação.	Considerado	A Matriz de Risco não é objeto de consulta pública, porém, os lapsos foram corrigidos.
BSO CONSULTING		
Inviabilidade do Prazo para Inventariação de Ativos (Artigo 32.º)	Parcialmente acolhido	Redação do artigo 32º alterada para acolher a alteração do prazo.
Proporcionalidade na Monitorização de "Entidades Importantes" (Anexo III)	Parcialmente acolhido	Medidas de cibersegurança mínimas adaptadas.

Conflito de Prazos e Operacionalidade na Resposta a Incidentes (Capítulo III)	Não acolhido	Ausência de norma habilitante para a alteração de prazos previstos no Decreto-Lei nº 125/2025.
Notificação eletrónica presume-se feita ao 3.º dia (Art. 19.º, n.º 4) propõe-se alargar para o 5.º dia útil.	Não acolhido	As notificações do artigo 19.º não devem ser confundidas com notificação de incidentes e as regras de contagem de prazos decorrem do Código do Procedimento Administrativo.
Eliminar a expressão 'por uma única vez'. Esta limitação viola o Princípio da Colaboração (Artigo 11.º do CPA) e o Princípio da Investigação e Verdade Material (Artigo 58.º do CPA). A qualificação de uma entidade é um ato de segurança nacional que não pode ser cerceado por formalismos que impeçam o pleno esclarecimento técnico. Art. 8.º, n.º 4	Não acolhido	O pedido único de informações adicionais às entidades após o preenchimento do requerimento visa garantir a celeridade processual.
O Regulamento deve garantir que a submissão no portal do CNCS desonera a entidade de outros reportes até à definição dos protocolos. Art. 4.º, n.º 3	Não acolhido	Incompatibilidade com o disposto no Decreto-Lei nº 125/2025.
Reduzir o prazo do Art. 27.º, n.º 5 para 72 horas e comunicar alterações em certificados.	Parcialmente acolhido	Redação do artigo 27º alterado quanto aos prazos.
Art. 9.º, n.º 4. Colisão com o RGPD. Se a lei não se aplica, a autoridade não deve reter dados técnicos/contactos sem consentimento. A conservação deve ser opcional (opt-in) e por solicitação expressa da entidade.	Não acolhido	O prazo legal de 5 anos previsto no Projeto de Regulamento é proporcional aos fins de interesse público de conservação dos dados a ter em conta. Não existe incompatibilidade com o Regulamento (UE) 679/2016, nem com a Lei nº 58/2019.
Art. 17.º, n.º 1. Redefinir como "Indisponibilidade Técnica". Prever canais offline ou via autoridades policiais.	Parcialmente acolhido	Redação do artigo 17º alterada, para adotar a expressão "indisponibilidade técnica".

ID.GA-1 e ID.GA-2- Exigência e proporcionalidade para Nível Básico	Não acolhido	As medidas de cibersegurança mínimas não exigem a utilização de ferramentas especificas para a realização do inventário.
Controlo PR.GA-3 – MFA e OT	Parcialmente acolhido	Medidas de cibersegurança mínimas alteradas.
Nível Substancial- Carga operacional e monitorização	Não acolhido	O Regulamento define as medidas mínimas de cibersegurança obrigatórias aplicáveis de forma abrangente, transversal e pretendendo abarcar o maior número de situações. A verificação da aplicação das medidas tem em conta o princípio da proporcionalidade.
Nível Elevado: Complexidade de Implementação (Controlo RS.AI-1)	Não acolhido	O Regulamento define as medidas mínimas de cibersegurança obrigatórias aplicáveis de forma abrangente, transversal e pretendendo abarcar o maior número de situações. A verificação da aplicação das medidas tem em conta o princípio da proporcionalidade.
Cloudflare		
Clarificar o que significa a "presunção de conformidade" concedida pela certificação ISO 27001.	Parcialmente acolhido	Redação do artigo 27º alterada. Quanto aos atos de supervisão, o contributo extravasa o âmbito do Regulamento.
Prazo de reporte de incidentes.	Não acolhido	Os detalhes quanto à notificação de incidentes serão definidos através de uma instrução técnica do CNCS, nos termos do disposto no nº4 do artigo 41º do Decreto-Lei n.º 125/2025.
Armazenamento de longo prazo de ficheiros como relatório anual, lista de ativos e relatórios de incidentes	Parcialmente acolhido	Redação do artigo 16º alterada.
Solicitamos que o CNCS considere qual o papel que a lista de ativos serve e contemple meios alternativos pelos quais este objetivo poderia ser alcançado sem a carga administrativa e os riscos associados à manutenção do requisito da lista de ativos.	Não acolhido	A lista de ativos é essencial para o zelo eficaz e pleno de uma cultura robusta de cibersegurança no contexto nacional, e a sua exigência não é excessivamente onerosa para as entidades.

GPCFA		
Convergência IT/OT e Segmentação Progressiva de Redes	Não acolhido	O Regulamento já respondeà necessidade de segregação de redes, a exigência de zero trust e à gestão de risco de ativos, incluindo *legacy* e OTs. Adicionalmente, as medidas pretendem ser o mais abrangentes possível.
Maturidade e Auditoria Escalonada na Cadeia de Abastecimento	Não acolhido	O Regulamento prevê medidas para os contratos com requisitos de cibersegurança a celebrar com a cadeia de abastecimento, numa lógica do princípio da proporcionalidade e de não retroatividade. Adicionalmente, as medidas que dispõem sobre os requisitos de cibersegurança dos contratos pretendem ser as mais abrangentes possíveis.
Diversidade Geográfica e OOBM (Redundância Lógica)	Não acolhido	O Regulamento prevê na medida PR.RI-4 que as entidades devam ter mecanismos que garantam a disponibilidade dos seus sistemas críticos, não definindo de que modo é que estes mecanismos devem ser implementados pelas entidades.
Automação M2M e Partilha de Ameaças com "Human-in-the-Loop"	Não acolhido	A notificação de incidentes é feita pelas entidades, manualmente, na Plataforma eletrónica, ou através da comunicação interoperável entre as entidades e a plataforma. Adicionalmente, o Regulamento prevê uma medida no DE.MC-7 quanto à gestão dos falsos positivos e decisões de bloqueio de código e/ou atividades maliciosas, que permitem que as entidades decidam como gerir estes eventos.
Autenticação MFA Resistente a Phishing (Abordagem Cirúrgica)	Não acolhido	O Regulamento define as medidas mínimas de cibersegurança, obrigatórias, podendo as entidades implementar medidas de cibersegurança mais exigentes em função da análise dos riscos de cibersegurança, nomeadamente, no que concerne a análise de gestão do risco residual.
Transição Pós-Quântica (PQC) e Inventariação	Não acolhido	O Regulamento define as medidas mínimas de cibersegurança, obrigatórias, podendo as entidades implementar medidas de cibersegurança mais exigentes em

		função da análise dos riscos de cibersegurança, nomeadamente, no que concerne a análise de gestão do risco residual.
Ciberseguro como Mecanismo de Transferência de Risco	Não acolhido	O Regulamento define as medidas mínimas de cibersegurança, obrigatórias, podendo as entidades implementar medidas de cibersegurança mais exigentes em função da análise dos riscos de cibersegurança, nomeadamente. Adicionalmente, cabe às entidades definir as medidas adequadas para tratamentos dos riscos.
Red Teaming e *Bug Bounty* em Modelos Controlados	Não acolhido.	O Regulamento define as medidas mínimas de cibersegurança, obrigatórias, podendo as entidades implementar medidas de cibersegurança mais exigentes em função da análise dos riscos de cibersegurança, nomeadamente, no que concerne a análise de gestão do risco residual.
Análise Anual de Lacunas de Capacidade (Engenharia Humana)	Não acolhido	O Regulamento define as medidas mínimas de cibersegurança, obrigatórias, podendo as entidades implementar medidas de cibersegurança mais exigentes em função da análise dos riscos de cibersegurança, nomeadamente, no que concerne a análise de gestão do risco residual. Caberá às entidades identificar as necessidades de formação em matéria de cibersegurança e definir o plano de formação adequado.
Integridade em Algoritmia e Inteligência Artificial	Não acolhido	O Regulamento define as medidas mínimas de cibersegurança, obrigatórias, podendo as entidades implementar medidas de cibersegurança mais exigentes em função da análise dos riscos de cibersegurança, nomeadamente, no que concerne a análise de gestão do risco residual.
APRITEL		
Clareza do artigo 6º quanto aos tipos de acessos possíveis à plataforma.	Acolhido	Redação do artigo 6º alterada.

Registo na plataforma de entidades inseridas em mais que um setor.	Considerado	Redação do artigo 8º alterada.
Esclarecimento do regime de qualificação do artigo 9.º.	Parcialmente acolhido	O prazo da notificação de qualificação decorre do nº5 do artigo 8º do Decreto-Lei n.º 125/2025. A redação do artigo 9º foi clarificada. O prazo de 90 dias para a extinção do registo provisório é proporcional às necessidades levantadas pelo procedimento de qualificação das entidades.
Comunicações com as autoridades de cibersegurança (artigo 12.º)	Não acolhido	As comunicações previstas no artigo 12.º englobam todos os atos relativos ao cumprimento das obrigações a que as entidades possam estar adstritas.
Modelos de apresentação do Relatório Anual-Consulta às entidades abrangidas.	Não acolhido	A consulta na elaboração dos modelos de apresentação do relatório anual está prevista no nº5 do artigo 30.º do Decreto-Lei n.º 125/2025.
Inconsistência dos prazos de comunicação do responsável de cibersegurança e ponto de contacto permanente	Acolhido	Redação dos artigos 14º e 15º alterada.
Designação do Responsável de Segurança e do Ponto de contacto permanente para os operadores de comunicações eletrónicas	Não acolhido	O contributo extravasa o âmbito do Regulamento.
Notificação simultânea de incidentes e partilha de informação automática entre autoridades.	Considerado	O contributo é pertinente e a questão foi tida em conta. O nº7 do artigo 40.º do Decreto-Lei n.º 125/2025 prevê a notificação simultânea de incidentes a várias autoridades.
Notificação de incidentes dos operadores de comunicações eletrónicas	Não acolhido	O contributo extravasa o âmbito do Regulamento
Natureza jurídica do QNRCS e dos anexos	Considerado	Redação clarificada
Aplicação conjunta QNRCS e medidas	Acolhido	Redação alterada
Certificação voluntária e dispensa/suavização dos requisitos de auditorias do artigo 54º	Não acolhido	A presunção de cumprimento das medidas de cibersegurança é ilidível, não desonerando as entidades das obrigações a que possam estar adstritas.

Matriz de risco e comunicação dos níveis de conformidade às entidades	Acolhido	Redação do aritgo 9º alterada.
Poderes do CNCS e imposição de certificações	Considerado	Redação do artigo 30º clarificada.
Gestão do risco residual pouco densificada quanto a metodologias, critérios de aceitação do risco e articulação entre os critérios previstos no n.º 5 do artigo 31.º e o disposto no Regulamento de Execução (UE) 2024/2690, de 17 de outubro de 2024	Parcialmente Acolhido	Redação do artigo 31º alterada.
Não é totalmente claro se a lista de ativos a comunicar ao CNCS se limita exclusivamente aos ativos diretamente acessíveis publicamente através da Internet. Prazo de submissão e conceito de "ativos essenciais".	Acolhido	Redação do artigo 32º alterada.
Densificação das obrigações relativas à cadeia de abastecimento.	Não acolhido	O artigo 28.º do Decreto-Lei n.º 125/2025 não carece de regulamentação. As densificações das medidas aplicáveis à cadeia de abastecimento encontram-se nas medidas de cibersegurança mínimas.
Nível Básico- ID.GA-5 Esclarecimento quanto à definição de ativos humanos, dados e tempo.	Parcialmente acolhido	Na medida ID.GA-5 foram retiradas as referências a ativos humanos e tempo.
Nível Básico- PR-GA-3: a exigência de autenticação multifator (MFA)	Acolhido	Redação alterada
Nível Básico- PR.SP-2: Recolha de *Logs*	Parcialmente acolhido	As entidades definirão o período de armazenamento com base na análise de risco e no princípio da proporcionalidade.
Nível Básico- DE.MC-1- Mecanismos de Proteção	Não acolhido	O Regulamento define as medidas mínimas de cibersegurança, obrigatórias, podendo as entidades implementar medidas de cibersegurança mais exigentes em função da análise dos riscos de cibersegurança.

Nível Substancial- GR.PP-1: Esclarecimento quanto à Política de Classificação e Gestão de Dados e requisitos mínimos	Não acolhido	O Regulamento define as medidas mínimas de cibersegurança, obrigatórias, podendo as entidades implementar medidas de cibersegurança mais exigentes em função da análise dos riscos de cibersegurança. Adicionalmente o CNCS irá proceder ao desenvolvimento de guias que irão auxiliar as entidades na aplicação das medidas de cibersegurança.
Nível Substancial- Clarificação do controlo ID.GA-4: As redes e sistemas de informação externos identificados e catalogados	Acolhido	Foram efetuadas alterações para acomodar o contributo.
Nível Substancial-PR.GA-1: Os ciclos de vida de gestão de identidades são definidos.	Não acolhido	A entidade define na sua Política de Gestão de Identidades, Autenticação e Controlo de Acessos quais os sistemas cujas credenciais devem ser desativadas após um período específico de inatividade. A medida não limita a monotorização dos sistemas críticos, seja interno ou externo. O critério de verificação não limita quais as evidências técnicas para demonstrar o cumprimento da medida. Cabe à entidade garantir que a evidência técnica cumpre com o disposto na medida.
Nível Substancial-PR.GA-5: A entidade aplica na sua gestão de acessos, os princípios do menor privilégio e da segregação de funções	Não acolhido	A medida está estruturada de forma abrangente e por isso inclui a revogação dos acessos remotos. Adicionalmente estão previstas outras medidas para a gestão dos acessos remotos. O critério de verificação não limita quais as evidências técnicas para demonstrar o cumprimento da medida. Cabe à entidade garantir que a evidência técnica cumpre com o disposto na medida.

Nível Substancial- PR.SD-5: São realizadas, mantidas e testadas cópias de segurança dos dados da entidade	Não acolhido	Cabe à entidade definir na Política de Cópias de Segurança a periodicidade o nível de exigência da realização das cópias de segurança. O critério de verificação não limita quais as evidências técnicas para demonstrar o cumprimento da medida. Cabe à entidade garantir que a evidência técnica cumpre com o disposto na medida.
Nível Substancial-.RI-3: Os ativos tecnológicos da entidade são protegidos de ameaças naturais	Não acolhido	O critério de verificação não limita quais as evidências técnicas para demonstrar o cumprimento da medida. Cabe à entidade garantir que a evidência técnica cumpre com o disposto na medida.
Nível Substancial-DE.MC-1: As redes e sistemas de informação são monitorizados para detetar potenciais incidentes	Acolhido	Foram efetuadas alterações para acomodar o contributo.
Nível Substancial-DE.MC-5: A utilização de aplicações não autorizadas em dispositivos móveis é detetada	Não acolhido	Entende-se que a Política de Uso Aceitável deve definir quais os requisitos para utilização de dispositivos móveis da entidade.
Nível Elevado-GR.CA-8: O Plano de Resposta a Incidentes e o Plano de Recuperação de Desastres são testados com o acompanhamento dos fornecedores	Não acolhido	As medidas não preveem que o pessoal-chave seja identificado individualmente.
Nível Elevado- DE.MC-1: As redes e sistemas de informação são monitorizados para detetar potenciais incidentes	Acolhido	Foram efetuadas alterações para acomodar o contributo. A medida não limita a monotorização dos sistemas críticos, seja interno ou externo.
Nível Elevado- DE.AE-1: Os eventos detetados são analisados	Não acolhido	Entende-se que o nível elevado deve requerer um sistema automatizado para agregação, correlação e análise dos eventos de segurança detetados.
Anexo IV - Medidas de Cibersegurança Mínimas para Entidades Públicas Relevantes	Não acolhido	As entidades públicas relevantes têm um regime de medidas menos exigentes que as entidades essenciais e importantes.
DSF		

Artigo 6º- Conta de utilizadores na plataforma.	Acolhido	Redação do artigo clarificada
Artigo 14º- "início de funções" do Responsável de Cibersegurança	Não acolhido	Contributo não percetível.
Artigo 17º- Situações de falência do sistema e inclusão do reigsto de receção.	Acolhido	Redação do artigo clarificada.
Anexo I QNRCS	Não acolhido	O Quadro Nacional de Referência para a Cibersegurança (QNRCS) não é objeto de consulta pública.
RS		
Requisitos para sistemas OT	Não acolhido	O Regulamento define as medidas mínimas de cibersegurança obrigatórias aplicáveis de forma abrangente, transversal e pretendendo abarcar o maior número de situações. A verificação da aplicação das medidas tem em conta o princípio da proporcionalidade.
Thales		
Normas de referência de sistemas OT	Não acolhido	O Regulamento define as medidas mínimas de cibersegurança obrigatórias aplicáveis de forma abrangente, transversal e pretendendo abarcar o maior número de situações. A verificação da aplicação das medidas tem em conta o princípio da proporcionalidade.
APB		
Necessidade de adequada articulação entre o Projeto de Regulamento e o quadro especial aplicável ao sector bancário (DORA / Lei n.º 73/2025), bem como de não duplicação dos requisitos a que ficam sujeitos os bancos nacionais	Parcialmente acolhido	Redação do artigo 10º alterada para acomodar parte do contributo.
Clarificações necessárias quanto ao funcionamento da plataforma eletrónica	Considerado	Redação do artigo 6º clarificada.
Título do Projeto de Regulamento	Acolhido	Lapso corrigido.

Artigo 3º- Definições- A remissão para a "alínea a) do n.º 2 do artigo 15.º" surge desacompanhada da identificação do diploma a que respeita,	Acolhido	Definição complementada.
Anexo I - Quadro Nacional de Referência em Cibersegurança (QNRCS)- Consulta Pública	Não acolhido	O Quadro Nacional de Referência para a Cibersegurança (QNRCS) não é objeto de consulta pública.
Anexo II – Matriz de Risco- Consulta Pública	Não acolhido	A Matriz de Risco não é objeto da consulta pública.
APED		
Designação do responsável de cibersegurança	Não acolhido	O "se aplicável" já traz clareza sobre o enquadramento normativo e quanto à base legal da designação.
Periodicidade das avaliações de risco- artigo 31º	Acolhido	Redação do artigo 31º alterada.
Definição de "Impacto Significativo"	Não acolhido	Será objeto de instrução técnica a definição dos parâmetros e limiares para definição de incidente de impacto significativo nos termos do nº4 do artigo 40º do Regime Jurídico da Cibersegurança.
Inventário de ativos e dependências	Acolhido	Foram efetuadas alterações para acomodar o contributo.
Critérios para o Exercício de Poderes de Supervisão Reforçada	Considerado	A redação do artigo 30º foi clarificada.
Risco de Fragmentação Regulatória	Não acolhido.	O disposto no n.º do artigo 20º do Decreto-Lei n.º 125/2025 para o qual o Regulamento remete prevê que a emissão de regulamentos setoriais pelas autoridades seja sempre precedida de um parecer do CNCS.
Carácter vinculativo do QNRCS	Parcialmente acolhido.	O Quadro Nacional de Referência para a Cibersegurança (QNRCS) não tem carácter vinculativo, como disposto no artigo 14.º do DL nº 125/2025. Os artigos 23.º, 24.º e 26.º do Regulamento foram alterados para clarificação da matéria.
Extensão Indireta do Regime Jurídico	Considerado	Redação do nº2 artigo 24º alterada.
Certificação ISO 27001 como Evidência de Conformidade	Acolhido	Redação alterada.

Observações sobre a Qualificação de Entidades Públicas como Entidades Essenciais	Não acolhido.	Nota-se que a Administração Pública, para efeitos da Matriz de Risco, é tida como setor.
Designação da Primeira coluna da tabela do Anexo III	Não acolhido	A designação da Primeira coluna da tabela é controlo de cibersegurança de acordo com a estrutura e terminologia do Quadro Nacional de Referência para a Cibersegurança (QNRCS).
Desalinhamento entre o PDF do CNCS e a Versão Publicada em Diário da República Anexo III	Acolhido	Foram efetuadas alterações para acomodar o contributo.
Entradas duplicadas Anexo III	Acolhido	Foram efetuadas alterações para acomodar o contributo.
Desalinhamento entre o Anexo III e o QNRCS	Acolhido	Foram efetuadas alterações para acomodar o contributo.
Lapsos de Remissão e de Construção Sintática	Acolhido	Lapsos corrigidos. O artgo 29º do Decreto-Lei tem numeração e por isso a mesma encontra-se referida no artigo 31º do Regulamento.
Lapsos de Numeração	Acolhido	Lapsos corrigidos.
Universidade do Minho		
Inventário de ativos expostos	Não acolhido	A lista de ativos é essencial para o zelo eficaz e pleno de uma cultura robusta de cibersegurança no contexto nacional, e a sua exigência não é prejudicial às entidades.
Nível Elevado: Complexidade de Implementação (Controlo RS.AI-1)	Não acolhido	O Regulamento define as medidas mínimas de cibersegurança obrigatórias aplicáveis de forma abrangente, transversal e pretendendo abarcar o maior número de situações. A verificação da aplicação das medidas tem em conta o princípio da proporcionalidade.
Siemens, SA		
Normas de referência de sistemas OT	Não acolhido	O Regulamento define as medidas mínimas de cibersegurança obrigatórias aplicáveis de forma abrangente, transversal e pretendendo abarcar o maior número de situações. A verificação da aplicação das medidas tem em conta o princípio da proporcionalidade.

APCER		
Aperfeiçoamento dos critérios de verificação	Não acolhido	Os critérios de verificação dos anexo III e IV são evidências factuais, documentais ou técnicas consideras adequadas pelas autoridades de cibersegurança competentes para evidenciar a implementação das medidas de cibersegurança. No entanto cabe a cada entidade definir a forma de implementação da medida de cibersegurança, cabendo às autoridades de cibersegurança competentes em sede de supervisão avaliar adequada implementação das medidas e o respetivo cumprimento do Regime Jurídico da Cibersegurança
Presunção de cumprimento do artigo 27º	Parcialmente acolhido	Foram efetuadas alterações para acomodar parcialmente o contributo.
FCD		
Comentários Projeto de Regulamento do Regime Jurídico de Cibersegurança	Não acolhido	Não configuram contributos para o Projeto de Regulamento.
IBERDROLA		
Coordenação real entre Estados-Membros para notificação, auditoria e resposta a incidentes	Não acolhido	Os contributos extravasam o âmbito do Regulamento.
Mandatos internos para registo e operação na plataforma por áreas corporativas (*shared services* do Grupo)	Não acolhido	Importa garantir que o acesso à área reservada das entidades é feito por quem tenha poderes para o efeito. Nessa medida, o n.º 3 do artigo 6.º do Projeto de Regulamento prevê já a possibilidade de concessão limitada de acessos.
Certificação e maturidade (ISO/IEC 27001)	Não acolhido	O disposto no contributo resulta já dos pressupostos do Regulamento.
Alinhamento com legislação equivalente de outros Estados-Membros (Ex.: Espanha/ENS):	Não acolhido	Extravasa o âmbito do Regulamento.
Homogeneidade e responsabilização (Supervisão centralizada no CNCS)	Não acolhido	Extravasa o âmbito do Regulamento.
Proporcionalidade setorial na energia ("Essencial" versus "Importante")	Não acolhido	Os critérios de qualificação resultam do Decreto-Lei n.º 125/2025 e não do Regulamento.
Câmara Municipal de Valongo		

Artigo 27º- Densificação conceitos da certificação voluntária	Parcialmente acolhido	Redação do artigo 27º alterada.
Artigo 20º- Notificação obrigatória- Administração Local	Não acolhido	Os prazos dispostos quanto à notificação de incidentes são definidos pelo Decreto-Lei n.º 125/2025, pelo que o Regulamento não pode criar prazos diferentes consoante o tipo de entidades.
Artigo 31º do Decreto-Lei n.º 125/2025- Responsável de Cibersegurança	Não acolhido	Extravasa o âmbito do Regulamento.
Criação da função pública de CISO	Não acolhido	Extravasa o âmbito do Regulamento.
AM Moura & Associados		
Ponto 2- Proposta para a adoção do regime simplificado	Não acolhido	Não acolhido, por implicar a derrogação do Decreto-Lei n.º 125/2025.
Ponto 3- Responsável de Cibersegurança e Ponto de Contacto Permanente	Não acolhido	Não foi acolhido, por resultar já do n.º 7 do artigo 31.º do Decreto-Lei n.º 125/2025.
Instituto de Informática da Segurança Social		
1-Periodicidade das Autoavaliações e Auditorias Internas	Não acolhido	O Regulamento define as medidas mínimas de cibersegurança obrigatórias aplicáveis de forma abrangente, transversal e pretendendo abarcar o maior número de situações. A verificação da aplicação das medidas tem em conta o princípio da proporcionalidade.
2-Modelo de Governo e Segregação de Funções na Plataforma MyCiber	Acolhido	Redação do artigo 6º alterada.
3-Clarificação da Não Responsabilização Automática da Entidade Notificante	Não acolhido	Não acolhido, por se tratar de matéria constante do Decreto-Lei n.º 125/2025.
4-Critérios de Aceitabilidade para Atrasos na Notificação de Incidentes	Não acolhido	Não acolhido por extravasar o âmbito do Regulamento.
5-Articulação e Primazia entre Autoridades Competentes	Não acolhido	Não acolhido por extravasar o âmbito do Regulamento.
6-Regime Transitório para Fornecedores e Contratos em vigor	Não acolhido	Não acolhido por extravasar o âmbito do Regulamento.
IGFEJ		

Matriz de Risco- Artigo 28º- Tendo em conta a Matriz definida, parece existir um vazio legal no que concerne ao cálculo do nível de conformidade e respetivas medidas mínimas de segurança a adotar pelas entidades.	Não acolhido	A Administração Pública, para efeitos da Matriz, é tida como setor.
Anexo II- Matriz de Risco- O artigo 28º, assim como também o Anexo II para onde este remete a definição da matriz, também não é claro sobre como será gerido o conjunto de cenários de risco (cenários de risco e atores) para obtenção do nível de conformidade. Serão as entidades a criar esses cenários, ou será o CNCS a disponibilizar? Será este tema clarificado no quadro que o CNCS "poderá" disponibilizar na plataforma (ponto 5)	Considerado	A Matriz de Risco não é alvo de consulta pública. O artigo 28º foi clarificado.
No artigo 31º não existe ponto 3, passa do 2 para o 4, pelo que o 4 deveria ser o 3	Acolhido	Lapso corrigido.
No artigo 33º existem dois pontos 3, devendo o segundo ser o 4.	Acolhido.	Lapso corrigido.
Transportes Metropolitanos de Lisboa		
Autoidentificação- Submissão documental e/ou espaço de fundamentação e prazo de decisão e exclusão de responsabilidade.	Considerado.	O formulário com base no disposto no artigo 8º do Regulamento que completa o disposto no artigo 35º do Decreto-Lei n.º 125/2025 assegura a recolha da informação necessária à qualificação.
Gestão de Contas e Acessos à Plataforma Eletrónica.	Considerado.	Redação do artigo 7º clarificada.
Registo (Transição de Dados- entre entidades abrangidas pelo Regime Jurídico revogado)	Não acolhido	Não configuram contributos para o Projeto de Regulamento. O Regime Jurídico da Segurança do Ciberespaço foi revogado.

NECHO TECH LAW		
Introdução de Responsável de Cibersegurança nas EPR	Não acolhido	Não acolhido, extravasa o âmbito do Regulamento.
Separação entre função de Governação e função operacional	Não acolhido	Matéria prevista no Decreto-Lei n.º 125/2025.
Requisitos Mínimos de Governação para as entidades públicas relevantes.	Não acolhido	O Regulamento define as medidas mínimas de cibersegurança obrigatórias aplicáveis de forma abrangente, transversal e pretendendo abarcar o maior número de situações. A verificação da aplicação das medidas tem em conta o princípio da proporcionalidade.
Modelo Estruturado de Evidência alinhado com QNRCS	Não acolhido	O contributo extravasa o âmbito do Regulamento.
Gestão do Risco Residual (Modelo Simplificado) para as entidades públicas relevantes	Não acolhido	O contributo extravasa o âmbito do Regulamento.
Eversheds Sutherland		
NIF- Responsável de Cibersegurança	Considerado	O CNCS emitirá oportunamente orientações técnicas quanto a esta matéria.
Designação de Responsável de Cibersegurança	Não acolhido	Não acolhido, extravasa o âmbito do Regulamento.
Entidades e dimensão	Não acolhido	Não acolhido, extravasa o âmbito do Regulamento.
Miranda Law Firm		
Alteração do teor do artigo 8.2 (a) do Projeto de Regulamento	Não acolhido	Não acolhido, por corresponder ao artigo 35.º do Decreto-Lei n.º 125/2025.
Hovione		
Questão Multi-country	Não acolhido	Não acolhido, extravasa o âmbito do Regulamento.
Restantes Questões	Não acolhidas	Não acolhido, por não implicar contributos ao regulamento.
NOS		
Identificação e acesso à plataforma eletrónica- O regime de acesso à plataforma não pode comprometer a sua operacionalização, devendo ser permitida a	Considerado	Importa garantir que o acesso à área reservada das entidades é feito por quem tenha poderes para o efeito. Nessa medida, o n.º 3 do artigo 6.º do Projeto de Regulamento prevê já a possibilidade de se poder conceder acessos limitados.

criação de perfis com diferentes permissões.		
Registo na Plataforma- Deve existir um registo único por entidade, independente do número de serviços prestados e autoridades competentes.	Considerado.	Redação do artigo 8º clarificada.
Qualificação de entidades- A responsabilidade pela qualificação deve ser do CNCS, em articulação com autoridades setoriais competentes.	Não acolhido	Não acolhido, uma vez que resulta já do Decreto-Lei n.º 125/2025.
Responsável de cibersegurança (artigo 14º) e ponto de contacto permanente (artigo 15º)- Os processos de designação e registo devem ser coerentes, permitindo aos operadores de comunicações eletrónicas manter designações específicas.	Parcialmente acolhido	Foram efetuadas alterações para acomodar parcialmente o contributo. O restante do contributo não é acolhido por extravasar o âmbito do Regulamento.
Obrigações de notificações de incidentes (artigo 20º)- Deve ser promovida a simplificação na notificação de incidentes, com utilização de uma plataforma única, responsável pela articulação e partilha de informação entre entidades.	Não acolhido	Contributo extravasa o âmbito do Regulamento.
QNRCS (23º)- As exigências de gestão do risco na cadeia de abastecimento devem ser calibradas ao impacto, criticidade e natureza dos fornecedores.	Não acolhido	As medidas de cibersegurança mínimas dispõem quanto à cadeia de abastecimento. Adicionalmente serão emitidas orientações para apoiar as entidades na implementação das medidas.
Âmbito aplicação do QNRCS (24º)- Normas setoriais específicas devem estar mapeadas com o QNRCS.	Considerado.	Contributo genérico.

Certificação voluntária (27º)- A certificação deve permitir a dispensa e/ou menores requisitos de auditorias periódicas.	Parcialmente acolhido	Parcialmente acolhido, tendo o contributo sido considerado na revisão do artigo 27.º
Exigência de certificação (30º)- Os critérios que permitem ao CNCS exigir certificações devem ser expressamente definidos, incluindo os prazos para adaptação a estas exigências.	Parcialmente Acolhido	Redação do artigo 30º alterada.
Gestão de risco residual (31º)- A análise de risco residual deve estar limitada aos ativos críticos. A avaliação de risco deve ser preventiva e adequada aos processos e realidade de cada organização.	Acolhido	Redação do artigo 31º clarificada e alterada para constar a análise e gestão do risco de cibersegurança e do risco residual.
Inventário de Lista de Ativos- Existem dúvidas sobre a pertinência dos elementos solicitados, sendo que a autoridade competente deve desenvolver capacidades para aferir eventuais riscos.	Não acolhido	A lista de ativos é essencial para o zelo eficaz e pleno de uma cultura robusta de cibersegurança no contexto nacional, e a sua exigência não é prejudicial às entidades.
ANA – Aeroportos de Portugal, S.A		
Redundância do n.º 1 do Artigo 23.º; n.º 3 do Artigo 23.; n. º1 do Artigo 28.º; n.º 5 do Artigo 30.º com o do Decreto-Lei n.º 125/2025	Considerados	As redundâncias mencionadas são intencionais e devem ser mantidas.
n.º 4 do Artigo 30 do Projeto de Regulamento	Considerado	Redação clarificada com a adição do nº6 no artigo 30º.
n.º 1 do Artigo 6.º do Projeto de Regulamento	Considerado	Redação alterada.
n.º 2 do Artigo 12.º do Projeto de Regulamento	Acolhido	Redação do Artigo 6 º alterada.
n.º 3 do Artigo 13. Projeto de Regulamento	Acolhido	Redação do Artigo 13 º alterada.
Artigo 14.º do Projeto de Regulamento	Acolhido	Lapso já corrigido.
Artigo 17.º do Projeto de Regulamento	Acolhido	Redação alterada.
Inclusão, no Projeto de Regulamento, de uma disposição com	Acolhido	Constava já do nº1 do artigo 84.º do Decreto-Lei n.º 125/2025, contudo redação do artigo 5.º do Projeto de

redação análoga à do refer ind.oº 3 do Artigo 1.º do Regulamento n.º 183/202		Regulamento alterada para garantir a redundância.
n.º 3 do Artigo 22.º e o n.º 5 do Artigo 28.º do Projeto de Regulamento	Acolhido	Redação dos artigos 22º e 28º alterada.
n.º 3 do Artigo 23.º e n.º 1 do Artigo 24.º do Projeto de Regulamento	Acolhido	Redação dos artigos 23º e 24º alterada.
n.º 1 do Artigo 24 do projeto de regulamento	Considerado.	Redação do artigo 24º alterada.
n.º 1 do Artigo 26.º Projeto de Regulamento	Considerado	Redação do artigo 26º alterada. .
n.º 3 do Artigo 27.º do Projeto de Regulamento	Não acolhido	A redação do artigo 27.º nº3 já prevê as recomendações levantadas.
Artigo 28.º e Anexo II do Projeto de Regulamento	Não acolhido	A Matriz não é objeto de consulta pública.
n.º 2 do Artigo 31. Do Projeto de Regulamento	Acolhido	Redação do artigo clarificada e alterada para constar a análise e gestão do risco de cibersegurança e do risco residual.
n.º 1 do Artigo 32.º do Projeto de Regulamento	Acolhido	Redação do artigo 32.º nº1 alterada.
PR.FC-2- O pessoal com funções especializadas em cibersegurança recebe formação adequada para o exercício das suas funções.	Acolhido	Redação alterada.
Artigos 14.º e 15. do Projeto de Regulamento	Não acolhido	O contributo extravasa o âmbito material do Projeto de Regulamento.
Lacuna estrutural crítica no Projeto de Regulamento	Não acolhido	O contributo extravasa o âmbito material do Projeto de Regulamento.
AGEFE		
Enquadramento e apreciação do tratamento dos endpoint devices	Não acolhido	O Quadro Nacional de Referência para a Cibersegurança (QNRCS) não é alvo de consulta pública.
Município de Barcelos		
Comentários à qualificação das entidades	Não acolhido	Matéria respeitante ao processo de qualificação das entidades, disposto no Decreto-Lei n.º 125/2025.
Aliança para a Cibersegurança		
Artigo 6.º Identificação e acesso à plataforma eletrónica- O n.º 1 e o n.º4 do artigo 6.º podem gerar alguma confusão às entidades abrangidas por este Regulamento.	Acolhido	Redação do artigo 6.º clarificada.

Artigo 12.º Comunicações com as autoridades de cibersegurança- Sem prejuízo para a existência do manual de utilização previsto no n.º 3, consideramos que o presente Regulamento deveria densificar requisitos mínimos para a configuração e segurança destas APIs.	Considerado	Redação do artigo 12.º clarificada.
Artigo 13.º Comunicação de documentos- Solicitamos, em relação a este ponto, uma clarificação sobre se estes modelos serão de aplicação obrigatória para todas as entidades ou se estas podem continuar a reportar de acordo com os seus próprios modelos e que tenham sido utilizados até agora, por exemplo, as entidades que já reportam ao abrigo do DORA.	Acolhido	Redação do artigo 13.º clarificada.
Artigo 15.º Ponto de contacto permanente- n.º 2 a) do artigo 15.º menciona que as entidades devem comunicar o "nome do elemento ou elementos da entidade que assume(m) a função de ponto de contacto permanente". No nosso entendimento, esta obrigação será de difícil cumprimento para entidades que tenham equipas de resposta a incidentes, por exemplo em modelo de SOC (Security Operations Center), a responder à função de ponto de contacto permanente, uma vez que estas equipas podem funcionar em 24x7 com elementos internos e externos, e onde o grau de	Não acolhido	Redação do artigo 15º alterada.

rotação pode ser elevado. Este fator poderá causar informação desatualizada com alguma regularidade.		
Artigo 17.º Situações de falência do sistema- No nosso entendimento, todo este enquadramento sobre segurança das comunicações e a proteção de informação confidencial endereçada no Regulamento n.º 183/2022 deve constar também do presente Regulamento.	Acolhido	Redação do artigo 17.º alterada.
Artigo 22.º Tramitação de notificações obrigatórias de incidentes- O n.º 3 do artigo 22.º coloca como possibilidade que a plataforma eletrónica possa disponibilizar mecanismos de emissão de alertas às entidades sobre os prazos previstos nos artigos 42.º a 44.º do Regime Jurídico da Cibersegurança. No nosso entendimento, este mecanismo, que seria uma grande mais-valia, apenas deve ser mencionado caso venha efetivamente a ficar disponível na plataforma eletrónica.	Acolhido	Redação do artigo 22º alterada
Artigo 26.º Aplicação conjunta- No nosso entendimento, a redação proposta para o n.º 2 do artigo 26.º pode gerar alguma confusão. Adicionalmente, também no n.º 2, são mencionadas descrições e orientações como fazendo parte do Anexo I, quando na proposta, o Anexo I não dispõe de orientações para cada um dos controlos, mas apenas descrições.	Acolhido	Lapso corrigido e redação do artigo 26º alterada.
Artigo 27.º Certificação voluntária- Sendo este um	Acolhido	Redação do artigo 27º alterada.

dos esquemas de certificação mais usados pelas entidades, solicitamos confirmação de que o critério de aceitação da certificação ISO/IEC 27001 será o âmbito da própria certificação, nomeadamente se o mesmo se aplica aos serviços essenciais prestados pelas entidades.		
Artigo 28.º Matriz de Risco- Assim, o n.º 4 deveria assegurar que são determinadas, de acordo com os cenários de riscos de cada setor, as medidas específicas do QNRCS e respetivo nível de conformidade para tratamento do cenário de risco.	Parcialmente acolhido	A redação do artigo 28º foi alterada.
Artigo 30.º nº4 Medidas de Cibersegurança Mínimas- O artigo 30.º, n.º 4, prevê a possibilidade do CNCS exigir certificações específicas, sem delimitar critérios materiais, condições procedimentais ou exigências mínimas de fundamentação, tendo impacto significativo em termos de custos e organização interna. Desta forma, consideramos que os critérios para a exigência de certificações devem ser expressamente definidos, incluindo prazos razoáveis para a adaptação às exigências (não inferior a 24 meses).	Considerado	A redação do artigo 30º foi alterada.
Artigo 31. º Gestão do Risco Residual- O n.º 1 do artigo 31.º prevê a abrangência da gestão de risco residual aos ativos que garantam a	Acolhido	Redação do artigo clarificada e alterada para constar a análise e gestão do risco de cibersegurança e do risco residual.

continuidade do funcionamento das redes e sistemas de informação que a organização utiliza.		
Artigo 32.º Lista de ativos publicamente acessíveis	Não acolhido	A lista de ativos é essencial para o zelo eficaz e pleno de uma cultura robusta de cibersegurança no contexto nacional, e a sua exigência não é prejudicial às entidades.
Nível Básico- GR.CO-4 e GR.CO-6 No nosso entendimento, esta medida de cibersegurança não deve incluir a obrigação de comunicar às partes interessadas externas quais são os serviços críticos, uma vez que se trata de informação confidencial, cujo acesso indevido externo poderá causar danos com impacto para a entidade.	Parcialmente Acolhido	Redação das medidas alteradas.
Nível Básico- ID.GA-5 Solicitamos informação adicional sobre a que se refere o ativo "tempo" ou retirar esta referência do Anexo III.	Acolhido	Redação alterada.
Nível Básico- GR.FR-4 Solicitamos informação adicional sobre o âmbito da Política de Uso Aceitável que é referido neste controlo e que a entidade deve definir e disponibilizar ao pessoal aquando da sua entrada.	Não acolhido	Entende-se que a Política de Uso Aceitável deve definir quais os requisitos para utilização de dispositivos móveis da entidade.
Nível Básico- GR.PP-1 Considerando que a Política é um documento de carácter estratégico e de alto nível, entende-se que pode não incluir detalhes específicos sobre funções e responsabilidades, motivo pelo qual tal exigência poderia ser reavaliada neste controlo.	Não acolhido	O Regulamento define as medidas mínimas de cibersegurança obrigatórias aplicáveis de forma abrangente, transversal e pretendendo abarcar o maior número de situações. A verificação da aplicação das medidas tem em conta o princípio da proporcionalidade.

Nível Básico- GR.GA-7- Foi identificada uma inconsistência na redação da medida de cibersegurança aplicável a este controlo ao mencionar que "a entidade deve efetuar avaliações do risco da cadeia de abastecimento pelo menos uma vez por ano ou sempre que relevante, no ambiente operacional, na cadeia de abastecimento". Adicionalmente, solicitamos esclarecimentos quanto ao significado de realizar avaliações de risco "no ambiente operacional" da cadeia de abastecimento.	Acolhido	Redação alterada.
Nível Básico- PR.FC-2- Este controlo determina que "o pessoal com funções especializadas em cibersegurança recebe formação adequada para o exercício das suas funções". Porém, a medida de cibersegurança está direcionada à formação dos membros dos órgãos de gestão, direção e administração, os quais, conforme nosso entendimento, não possuem funções especializadas em cibersegurança.	Acolhido	Redação alterada.
Nível Substancial- GR.CO-6 Sugerimos por isso que a componente relacionada à comunicação seja excluída do controlo, permanecendo apenas: "Os serviços externos, dos quais a entidade depende, são identificados."	Acolhido	Redação alterada no Nível Básico.
Nível Substancial- GR.PP-1 Este controlo aborda	Não acolhido	O Regulamento define as medidas mínimas de cibersegurança

políticas para a gestão da cibersegurança, incluindo a Política de Cibersegurança, contudo, a medida de cibersegurança refere-se especificamente à definição, aprovação e implementação de uma Política de Classificação e Gestão de Dados.		obrigatórias aplicáveis de forma abrangente, transversal e pretendendo abarcar o maior número de situações. A verificação da aplicação das medidas tem em conta o princípio da proporcionalidade.
Nível Substancial- ID.GA-6- A identificação de metadados não deve ser considerado controlo do nível substancial.	Acolhido	Redação alterada para o nível Elevado.
Nível Substancial- ID.AR-7- No nosso entendimento, o processo de gestão de vulnerabilidades da entidade não precisa, necessariamente, de estar alinhado com a referida política, mas sim contemplar a possibilidade de comunicação de vulnerabilidades ao CERT.PT, enquanto entidade coordenadora nacional para efeitos de divulgação coordenada.	Não acolhido.	O Regulamento define as medidas mínimas de cibersegurança obrigatórias aplicáveis de forma abrangente, transversal e pretendendo abarcar o maior número de situações. A verificação da aplicação das medidas tem em conta o princípio da proporcionalidade.
Nível Substancial- RS.NC-1- Na nossa opinião, a comunicação desses incidentes para stakeholders externos deve observar rigorosamente os requisitos previstos na legislação aplicável, e ser gerida pela organização com base no princípio da necessidade de conhecimento das partes interessadas externas.	Não acolhido.	Regulamento define as medidas mínimas de cibersegurança obrigatórias aplicáveis de forma abrangente, transversal e pretendendo abarcar o maior número de situações. A verificação da aplicação das medidas tem em conta o princípio da proporcionalidade
Nível Substancial- RC.CO-1-No nosso entendimento, a comunicação com stakeholders externos deve observar rigorosamente os requisitos previstos na legislação aplicável, e ser	Não acolhido.	Regulamento define as medidas mínimas de cibersegurança obrigatórias aplicáveis de forma abrangente, transversal e pretendendo abarcar o maior número de situações. A verificação da aplicação das medidas

gerida pela organização com base no princípio da necessidade de conhecimento das partes interessadas externas.		tem em conta o princípio da proporcionalidade
Nível Elevado-PR.GA-3 A medida de cibersegurança referida neste controlo aparenta não estar alinhada com o objetivo previsto no próprio controlo.	Não acolhido	O título do controlo é mais genérico e é abrangente o suficiente para ser aplicado por todas as entidades. Pelo contrário, as medidas mínimas de cibersegurança densificam o controlo, criando uma obrigatoriedade de aplicação que poderá revelar-se ou não mais restrita do que o próprio controlo.
DIGI |NOWO		
Quadro Nacional Referência para Cibersegurança-Com esse objetivo, entendemos que será fundamental que as autoridades relevantes, nomeadamente o CNCS e a ANACOM, publiquem um mapeamento oficial entre os requisitos do novo regime e os do Regulamento SIRSCE, que deverá ter um nível de detalhe que permita relacionar diretamente as medidas de cibersegurança do QNRCS e outros requisitos previstos no articulado do Projeto de Regulamento com as equivalentes medidas de segurança dos vários objetivos de segurança e outros requisitos do articulado do Regulamento SIRSCE.	Não acolhido	O contributo extravasa o Regulamento.
Análise de Risco e Matriz de Risco- Assim, sugere-se que seja definido um nível mínimo de criticidade para os alertas e incidentes que exijam a revisão da análise de risco.	Não acolhido	A Matriz de Risco não é alvo de consulta pública.
Inventário de ativos- O Projeto de Regulamento	Não acolhido	A realização do inventário de ativos pelas entidades é exigida nas medidas

exige, no seu artigo 32º, que as entidades devem elaborar, manter atualizado e comunicar à autoridade de cibersegurança competente uma lista de ativos, essenciais para a prestação dos respetivos serviços, que estejam diretamente acessíveis publicamente através da Internet. É exigido, ainda, em vários dos controlos de segurança do QNRCS a inventariação de ativos críticos da entidade.		mínimas de cibersegurança. Nesse sentido, a lista de ativos do artigo 32º do Regulamento terá por base o inventário de ativos já exigido em sede de medidas mínimas.
Notificação de incidentes e reporte de ocorrências excecionais - Assim, sugere-se que sejam definidos previamente, por acordo entre os Reguladores/Autoridades relevantes e as entidades, os templates dos relatórios a fornecer sobre ocorrências excecionais, nomeadamente, incêndios florestais, tempestades, cheias, falhas de energia e pandemias.	Não acolhido	O CNCS irá emitir uma instrução técnica nos termos do nº4 do artigo 40º.
Auditorias e certificação- Assim, entendemos que o nível de exigência e as metodologias seguidas nestas auditorias devem ser considerados equivalentes a um processo de certificação, pelo que, para efeitos do nº 3 do artigo 27º deve ser admitida a apresentação de um relatório de auditoria, eventualmente acompanhado de um plano de resolução de não conformidades já concluído.	Não acolhido	Não acolhido por contrariar o disposto no artigo 34.º nº3 do Decreto-Lei n.º 125/2025.

EDP		
Artigo 6º- Acessos à plataforma- A redação atual suscita dúvidas quanto ao modelo de gestão de acessos à plataforma eletrónica, conjugando a noção de conta única por entidade com a possibilidade de múltiplos utilizadores e responsáveis.	Acolhido	Redação do artigo 6º alterada.
Artigos 12º e 17º- Requisitos de segurança para comunicações- O Regulamento deve densificar os requisitos de segurança aplicáveis às comunicações realizadas fora da plataforma eletrónica, nomeadamente em situações de falência do sistema.	Acolhido	Redação dos artigos 12º e 17º alterada.
Artigo 13º- Caráter vinculativo dos modelos de reporte	Acolhido	Redação do artigo 13º alterada.
Artigo 14º e 15º- Inconsistências entre o RJC, o Regulamento e a operacionalização	Considerado	Redação dos artigos 14º e 15º aclarada.
Artigos 22ºe 28º- As referências a funcionalidades como mecanismos automáticos de alerta ou quadros de apoio à leitura da matriz de risco deverão constar do Regulamento apenas se tais funcionalidades estiverem efetivamente implementadas.	Acolhido	Redação dos artigos 22º e 28º alterada.
Artigo 24º- O QNRCS deverá manter o seu caráter de referência e orientação, não configurando uma obrigação de aplicação integral, em especial para entidades que já comprovem um nível adequado de maturidade	Acolhido	Redação do artigo 24º alterada.

através de certificações reconhecidas.		
Artigos 23.º, 26.º e 27.º- Os artigos devem reforçar de forma coerente que: O QNRCS não constitui, por si só, um esquema de certificação; A presunção de conformidade deve assentar em critérios objetivos e transparentes; Deve ser promovida a racionalização de auditorias, evitando sobreposição entre auditorias regulatórias e de certificação; As obrigações de comunicação relativas a certificados devem focar-se em situações materialmente relevantes (suspensão, revogação, renovação).	Parcialmente acolhido	Redação dos artigos 23º, 26º e 27º alterada.
Artigo 30º- Deve ser expressamente salvaguardada a possibilidade de adoção de medidas equivalentes às medidas mínimas, com base em esquemas de certificação reconhecidos.	Não acolhido	O disposto no artigo 27º do Regulamento já prevê a possibilidade de uma presunção de cumprimento de medidas cibersegurança previstas nos artigos 26º a 29º do Decreto-Lei n.º 125/2025 e 30º do Regulamento, através dos esquemas de certificação elencados no nº3 do artigo 27º do Regulamento. Porém, a redação do artigo 30º foi alterada.
Artigo 31º- Neste enquadramento, considera-se essencial que o Regulamento não condicione a gestão do risco residual a uma abordagem exclusivamente baseada em ativos, devendo permitir explicitamente metodologias que partam dos processos, serviços ou funções críticas, assegurando simultaneamente a	Acolhido	Redação do artigo 31º clarificada e alterada para constar a análise e gestão do risco de cibersegurança e do risco residual.

identificação e tratamento dos ativos subjacentes.		
Artigo 32º- Ativos publicamente acessíveis -O nível de detalhe atualmente exigido suscita preocupações relevantes quanto à proporcionalidade e à segurança da informação.	Não acolhido	A lista de ativos é essencial para o zelo eficaz e pleno de uma cultura robusta de cibersegurança no contexto nacional, e a sua exigência não é prejudicial às entidades.
Medidas de Cibersegurança Mínimas – Anexo III	Parcialmente acolhido	Redação alterada em alguns dos pontos.
E-Redes		
Artigo 6º-Identificação e acesso à plataforma eletrónica-A E-REDES sugere que seja clarificado como é que as entidades poderão fazer a gestão das contas e perfis de acesso à plataforma, quem terá o acesso inicial e como podem ser atribuídas contas e perfis a outros responsáveis da entidade, nomeadamente ao responsável de cibersegurança ou à pessoa ou pessoas que assegurem as funções de ponto de contacto permanente.	Considerado	Redação do artigo 6º alterada.
Artigo 8º- Lapso-Assinala-se um lapso de formatação no n.º 4 do artigo 8.º em "(…) mecanismos de interoperabilidades previstos no n.º 1 do artigo 87.º do RSC, , a autoridade de cibersegurança (…)".	Acolhido	Lapso corrigido.
Artigo 12º-Comunicações com as autoridades de cibersegurança-Apesar do n.º 3 do mesmo artigo mencionar que o CNCS disponibiliza um manual de utilização de cada interface de programação de aplicações, consideramos que o presente Regulamento	Parcialmente acolhido	Redação do artigo 12º alterada.

deve densificar os requisitos mínimos das APIs no próprio texto normativo, deixando o manual apenas para outros detalhes técnicos. Adicionalmente, também consideramos importante clarificar como é que esta possibilidade se alinha com o previsto no n.º 1 do artigo 7.º em que a autenticação na plataforma eletrónica é efetuada com recurso a sistema de identificação eletrónico com nível de garantia elevado.		
Artigo 13º- Modelos de comunicação de documentos - Reconhecendo a utilidade destes modelos para as entidades que estavam fora do âmbito de aplicabilidade da Diretiva NIS1 e que apenas agora vão começar a reportar o seu relatório anual, era importante clarificar se estes modelos serão de aplicação obrigatória para todas as restantes entidades ou se estas podem continuar a reportar de acordo com os seus próprios modelos e que têm sido utilizados até agora.	Acolhido	Redação do artigo 13º alterada.
Artigo 15º-Elementos quanto ao Ponto de Contacto Permanente - Neste sentido, a E-REDES sugere que seja mantida a redação da alínea a) do n.º 2 do artigo 2.º do Regulamento n.º 183/2022 que configura instrução técnica relativa a comunicações entre as entidades e o Centro	Acolhido	Redação do artigo 15º alterada.

Nacional de Cibersegurança, onde refere apenas "Nome da Entidade" ou, em alternativa, "Nome da função".		
Artigo 17º- Falência do sistema-A E-REDES sugere que os controlos relativos à segurança das comunicações e proteção de informação confidencial façam parte também do presente Regulamento. Também consideramos positivo que este artigo defina concretamente qual o endereço de correio eletrónico ou contacto telefónico que as entidades devem utilizar para comunicar informações em caso de falência do funcionamento da plataforma eletrónica.	Parcialmente Acolhido	Redação do artigo 17º alterada.
Artigo 22º- Notificações obrigatórias de incidentes-No entendimento da E-REDES, este mecanismo poderia ser de elevado valor para o cumprimento das obrigações de notificação de incidentes por parte das entidades, pelo que consideramos que o mesmo não deve estar mencionado como uma hipótese.	Acolhido	Redação do artigo 22º alterada.
Artigo 23º- Âmbito de aplicação QNRCS-No entendimento da E-REDES, este artigo deve prever uma matriz de equivalência do QNRCS com esquemas de certificação de referência existentes, tal como previsto no n.º 1 do artigo 34.º do Decreto-Lei n.º 125/2025, de 4 de	Acolhido	Redação do artigo 23º alterada.

dezembro, de forma que as entidades possam demonstrar o cumprimento das práticas existentes em matéria de gestão da cibersegurança e da segurança informação previstas no QNRCS através das certificações que já detêm.		
Artigo 24º- Âmbito de aplicação QNRCS-No n.º 1 do artigo 24.º refere que "o QNRCS é aplicável às entidades essenciais, importantes e públicas relevantes (…)" o que no entendimento da E-REDES apresenta um sentido de obrigação na aplicação do QNRCS que vai para além do que está previsto no Decreto-Lei n.º 125/2025, de 4 de dezembro.	Acolhido	Redação do artigo 24º alterada.
Artigo 25º- Estrutura do QNRCS-No n.º 1 do artigo 25.º refere que o QNRCS é estruturado em função do ciclo de vida da gestão da cibersegurança a realizar pelas entidades, mas não indica quais são estas entidades. Sugerimos neste artigo a concretização do n.º 1, nomeadamente se é aplicável às entidades essenciais e importantes ou também às entidades públicas relevantes.	Não acolhido	O artigo 25º dispõe quando à estrutura do QNRCS e não a sua aplicação nos termos do disposto nos artigos 23º e 24º para implementação das medidas mínimas.
Artigo 26º- Aplicação conjunta-Sendo o Anexo I do presente Regulamento o próprio QNRCS, não conseguimos entender o objetivo do n.º 2 do artigo 26.º ao referir que "a aplicação do QNRCS, enquanto instrumento nacional de referência e no	Acolhido	Redação do artigo 26º alterada.

âmbito da adoção de medidas de cibersegurança aplicáveis, pode ter em conta os controlos de cibersegurança e as suas respetivas descrições e orientações, constantes do Anexo I ao presente Regulamento"		
Artigo 27º- Certificação voluntária-No nosso entendimento, o incentivo à certificação para comprovar o cumprimento das medidas de cibersegurança é muito positivo e deveria ser tido em conta para gerir os requisitos das auditorias previstas no artigo 54.º do Decreto-Lei n.º 125/2025, de 4 de dezembro, nomeadamente a necessidade da sua execução, uma vez que as entidades já estão sujeitas a um grande esforço com a realização das auditorias de certificação.	Parcialmente acolhido	Redação do artigo 27º aclarada.
Artigo 28º- Matriz de Risco-No entendimento da E-REDES, este quadro de apoio poderia ser de elevado valor para as entidades pelo que consideramos que o mesmo não deve ser mencionado como uma hipótese.	Acolhido	Redação do artigo 28º alterada.
Artigo 30º- Medidas de Cibersegurança Mínimas-No nosso entendimento é importante salvaguardar que as entidades podem aplicar medidas equivalentes às medidas de cibersegurança mínimas tendo em conta uma matriz de equivalência do QNRCS com esquemas de	Parcialmente acolhido.	O disposto no artigo 27º do Regulamento já prevê a possibilidade de uma presunção de cumprimento de medidas cibersegurança previstas nos artigos 26º a 29º do Decreto-Lei n.º 125/2025 e 30º do Regulamento, através dos esquemas de certificação elencados no nº3 do artigo 27º do Regulamento. A redação do nº4 do artigo 30º foi alterada.

certificação de referência existentes.		
Artigo 31º- Gestão de Risco Residual-Da leitura do n.º 1 e n.º 2 deste artigo concluímos que não fica prevista nenhuma periodicidade para a análise e gestão dos riscos residuais em caso de não se verificar nenhum dos cenários previstos no n.º 2, ao contrário do que está definido no n.º 1 do artigo 10.º do Decreto-Lei n.º 65/2021 onde as análises dos riscos de âmbito global são realizadas pelo menos uma vez por ano.	Acolhido	Redação do artigo clarificada e alterada para constar a análise e gestão do risco de cibersegurança e do risco residual.
Artigo 32º-Propomos que este artigo seja revisto para exigir apenas informações estritamente necessárias à supervisão e apoio operacional do CNCS, detalhando a finalidade do tratamento de cada categoria de dados e as garantias de proteção aplicáveis.	Não acolhido	A lista de ativos é essencial para o zelo eficaz e pleno de uma cultura robusta de cibersegurança no contexto nacional, e a sua exigência não é prejudicial às entidades.
Artigo 33º-Por outro lado, no que concerne às medidas de bloqueio e redireccionamento, sendo adotadas em contexto excecional, o mesmo deveria ser acompanhado de parâmetros e critérios de aplicação mais objetivos, de forma a neutralizar o grau de discricionariedade.	Não acolhido	Já acautelado no nº4 do mesmo artigo.
Básico-GR.CO-4-Esta medida de cibersegurança não deve incluir a obrigação de comunicar às partes interessadas externas quais são os serviços críticos	Acolhido	Redação alterada
Básico- GR.CO-6- Esta medida de cibersegurança	Não acolhido	A medida apenas refere que a comunicação deve ser feita às partes

não deve incluir a obrigação de comunicar às partes interessadas externas quais são os serviços críticos		interessadas, não explícita às partes interessadas externas.
Básico- ID.GA-5- A medida de cibersegurança pode considerar os ativos humanos, mas não de forma discricionária como os restantes ativos, mas sim como funções e quantidades que podem representar riscos para a organização.	Acolhido	Redação alterada
Básico- GR.FR-4- A respetiva medida de cibersegurança refere que "a entidade deve definir uma Política de Uso Aceitável, disponibilizá-la ao pessoal aquando da sua entrada, sensibilizando-os para garantir o cumprimento da mesma", mas não diz o âmbito a que se aplica esta Política.	Acolhido	Redação alterada
Básico- GR.PP-1- A respetiva medida de cibersegurança refere que a Política de Cibersegurança aprovada pelos órgãos de gestão, direção e administração deve incluir a identificação e atribuição de funções e responsabilidades.	Não acolhido	O Regulamento define as medidas mínimas de cibersegurança obrigatórias aplicáveis de forma abrangente, transversal e pretendendo abarcar o maior número de situações. A verificação da aplicação das medidas tem em conta o princípio da proporcionalidade.
Básico- GR.CA -7- Assinala-se um lapso na redação da medida de cibersegurança aplicável neste controlo, quando refere que "a entidade deve efetuar avaliações do risco da cadeia de abastecimento pelo menos uma vez por ano ou sempre que relevante, no ambiente operacional, na cadeia de abastecimento".	Acolhido	Redação alterada

Adicionalmente, solicitamos mais informações sobre o que se entende por efetuar avaliações de risco "no ambiente operacional" da cadeia de abastecimento.		
Básico- PR.GA-1- Assinala-se um lapso de redação em "Evidência técnicas".	Acolhido	Lapso corrigido.
Básico- PR.FC-2- Este controlo refere que "o pessoal com funções especializadas em cibersegurança recebe formação adequada para o exercício das suas funções", no entanto a medida de cibersegurança remete para formação aos membros dos órgãos de gestão, direção e administração que, no nosso entendimento, não são as pessoas com funções especializadas em cibersegurança.	Acolhido	Redação alterada
Substancial GR.CO-06- O controlo refere que os serviços externos, dos quais a entidade depende, devem ser comunicados, mas a medida de cibersegurança não explica como é que essa comunicação se aplica.	Acolhido	Redação alterada para Nível Básico.
Substancial GR.PP-1- No nosso entendimento deve haver alinhamento entre o carácter genérico do controlo em relação a políticas de cibersegurança e a medida de cibersegurança que fala em matérias específicas a serem tratadas em Políticas.	Não acolhido	O título do controlo é mais genérico e é abrangente o suficiente para ser aplicado por todas as entidades. Pelo contrário, as medidas mínimas de cibersegurança densificam o controlo, criando uma obrigatoriedade de aplicação que poderá revelar-se ou não mais restrita do que o próprio controlo.
Substancial ID.GA-6- A identificação de metadados não deve fazer parte do	Acolhido	Redação alterada no Nível Elevado.

nível substancial tendo em conta os requisitos legais específicos e a complexidade da sua identificação/tratamento pela maioria das organizações. No máximo, deveria estar no nível Elevado.		
Substancial ID.AR-7- No nosso entendimento, o processo de gestão de vulnerabilidades da entidade não necessita de estar alinhado com a Política Nacional de Divulgação Coordenada de Vulnerabilidades, mas apenas prever que uma vulnerabilidade possa ser comunicada ao CERT.PT enquanto entidade coordenadora nacional para efeitos da divulgação coordenada de vulnerabilidades.	Parcialmente acolhido	A referência foi alterada para Instrução Técnica sendo que a mesma será publicada pelo CNCS. O Regulamento define as medidas mínimas de cibersegurança obrigatórias aplicáveis de forma abrangente, transversal e pretendendo abarcar o maior número de situações. A verificação da aplicação das medidas tem em conta o princípio da proporcionalidade.
Substancial RS.NC-1- No nosso entendimento, a comunicação de incidentes com partes interessadas externas deve ter em conta os requisitos definidos na legislação aplicável e deve ser gerida pela entidade numa base da necessidade de conhecimento pela parte interessada externa.	Não acolhido	Regulamento define as medidas mínimas de cibersegurança obrigatórias aplicáveis de forma abrangente, transversal e pretendendo abarcar o maior número de situações. A verificação da aplicação das medidas tem em conta o princípio da proporcionalidade
Substancial RC.CO-1- No nosso entendimento, a comunicação com partes interessadas externas deve ter em conta os requisitos definidos na legislação aplicável e deve ser gerida pela entidade numa base da necessidade de conhecimento pela parte interessada externa.	Não acolhido	Regulamento define as medidas mínimas de cibersegurança obrigatórias aplicáveis de forma abrangente, transversal e pretendendo abarcar o maior número de situações. A verificação da aplicação das medidas tem em conta o princípio da proporcionalidade
Elevado GR.FR-1- Assinala-se um lapso de numeração uma vez que	Acolhido	Redação alterada

este controlo aparece repetido 2 vezes, na linha 1 e linha 3 da tabela para o Nível Elevado.		
Elevado GR.SP-2- Assinala-se um lapso de numeração uma vez que este controlo aparece repetido 2 vezes, na linha 2 e linha 4 da tabela para o Nível Elevado.	Acolhido	Redação alterada
Elevado ID.MC-2- Assinala-se um lapso de numeração uma vez que este controlo aparece repetido 2 vezes.	Acolhido	Redação alterada
Elevado PR.GA-3- A medida de cibersegurança deste controlo parece não corresponder com o objetivo do controlo.	Não acolhido	O título do controlo é mais genérico e é abrangente o suficiente para ser aplicado por todas as entidades. Pelo contrário, as medidas mínimas de cibersegurança densificam o controlo, criando uma obrigatoriedade de aplicação que poderá revelar-se ou não mais restrita do que o próprio controlo.
CTT		
Artigo 1º- O artigo define de forma clara o âmbito do Regulamento, mas não explicita de forma suficiente os princípios orientadores da sua aplicação, em particular no que respeita à proporcionalidade e à abordagem baseada no risco, essenciais à correta implementação do Regime Jurídico da Cibersegurança.	Não acolhido	O artigo 1º assegura os objetivos propostos.
Artigo 4º- O artigo enumera funcionalidades da plataforma eletrónica, mas não define requisitos mínimos de disponibilidade, resiliência ou continuidade do serviço, elementos essenciais para o cumprimento das	Não acolhido	O contributo não carece de previsão no presente Regulamento.

obrigações legais associadas às notificações obrigatórias.		
Artigo 5º- Reforçar, no artigo, os princípios de continuidade de serviço da plataforma eletrónica, incluindo regras claras sobre a comunicação de indisponibilidades planeadas, bem como a definição de medidas de salvaguarda operacional aplicáveis em situações de exceção, assegurando previsibilidade e resiliência do modelo de comunicação.	Considerado	A matéria do contributo resulta já das normas do CPA, nomeadamente o seu nº2 do artigo 14.º, devidamente referidas no Projeto de Regulamento. Redação do artigo 17.º do presente Projeto de Regulamento alterada.
Artigo 6º- Os n.os 1 e 4 do artigo 6.º podem suscitar ambiguidades quanto ao modelo de gestão de acessos à plataforma eletrónica, em particular no que respeita à criação, gestão e eliminação de utilizadores	Considerado	Clarificação da redação do artigo 6º.
Artigo 8º- O nível de detalhe exigido no formulário de autoidentificação é elevado, podendo implicar a recolha de dados que já se encontram disponíveis em bases de dados da Administração Pública, bem como aumentar o risco de erro ou inconsistência na informação submetida. Esta situação traduz-se num acréscimo desnecessário da carga administrativa para as entidades e pode comprometer a qualidade, uniformidade e fiabilidade dos dados registados.	Não acolhido	Situação prevista no artigo 18.º do Regulamento.

Artigo 9º-O artigo prevê a possibilidade de alteração da qualificação das entidades "a qualquer momento", por decisão da autoridade de cibersegurança competente.	Não acolhido	Situação prevista no nº8 do artigo 26.º do Decreto-Lei n.º 125/2025.
Artigo 12º-A concentração de todas as comunicações na plataforma eletrónica cria uma elevada dependência operacional de uma infraestrutura única. Em cenários indisponibilidade da plataforma, esta dependência pode traduzir-se numa vulnerabilidade operacional relevante, afetando a capacidade das entidades cumprirem atempadamente as suas obrigações legais. Considera-se que o artigo carece de maior clarificação quanto aos requisitos técnicos aplicáveis às APIs.	Considerado	Redação do artigo 12º clarificada.
Artigo 13º-O n.º 3 do artigo 13.º não clarifica se os modelos de relatório a disponibilizar pelo CNCS têm carácter obrigatório ou meramente indicativo, o que poderá gerar incerteza quanto à admissibilidade de modelos próprios já utilizados por entidades com sistemas de reporte consolidados.	Acolhido	Redação do artigo 13º alterada.
Artigo 15º-A alínea a) do n.º 2 do artigo 15.º refere-se à identificação do ponto de contacto permanente, mas a redação atual parece pressupor implicitamente a designação de um ou mais	Acolhido	Redação do artigo 15º alterada.

indivíduos identificados nominalmente.		
Artigo 16º-O artigo 16.º estabelece um prazo geral de conservação de dados pessoais de cinco anos após a extinção do registo, sem explicitar a respetiva fundamentação nem distinguir entre diferentes tipologias de dados. Este prazo pode revelar-se excessivamente amplo, em particular para dados como contactos pessoais, e suscita dúvidas quanto à sua conformidade com o princípio da minimização e da limitação da conservação previsto no RGPD. A ausência de justificação clara para a adoção deste prazo único dificulta a sua compreensão e aplicação pelas entidades.	Não acolhido	O prazo legal de 5 anos previsto no Projeto de Regulamento é proporcional aos fins de interesse público de conservação dos dados a ter em conta. Não existe incompatibilidade com o Regulamento (UE) 679/2016, nem com a Lei nº 58/2019.
Artigo 17º-O artigo 17.º prevê mecanismos de contingência para situações de falência da plataforma eletrónica, baseados essencialmente no envio de informação por correio eletrónico ou no contacto telefónico. Contudo, a redação não explicita as medidas de segurança aplicáveis à utilização destes meios alternativos, nem os requisitos mínimos de autenticação, confidencialidade, integridade e rastreabilidade da informação transmitida.	Considerado	Redação do artigo 17º alterada.
Artigo 20º - Verifica-se um alinhamento formal do artigo 20.º com o Regime Jurídico da Cibersegurança; contudo,	Não acolhido	A notificação é sempre realizada à autoridade de cibersegurança do competente podendo ser uma das entidades da alínea a) do nº2 do artigo

subsistem riscos relevantes de divergência interpretativa do conceito de "impacto significativo", bem como uma complexidade acrescida na articulação entre as notificações inicial, intercalar e final. Acresce que a redação atual não clarifica de forma suficiente como é assegurada a articulação entre as várias entidades envolvidas no processo de notificação, nomeadamente o CNCS e outras autoridades competentes, o que pode conduzir a duplicação de reportes e a uma sobrecarga operacional significativa para as entidades obrigadas a notificar, sem acréscimo proporcional de valor para a gestão do incidente.		15º do Regime Jurídico da Cibersegurança. Será adicionalmente objeto de instrução técnica a definição dos parâmetros e limiares para definição de incidente de impacto significativo nos termos do nº4 do artigo 40º do Regime Jurídico da Cibersegurança.
Artigo 22º -O n.º 3 do artigo 22.º prevê de forma facultativa a disponibilização de alertas sobre os prazos legais de notificação. Atendendo à criticidade destes prazos, a natureza opcional desta funcionalidade pode comprometer a eficácia do regime e gerar assimetrias no seu cumprimento entre entidades.	Acolhido	Redação do artigo 22º alterada.
Artigo 23º-O n.º 3 do artigo 23.º refere que as entidades aplicam o QNRCS numa perspetiva de melhoria contínua, mas a redação atual não clarifica se a aplicação do QNRCS é exclusiva ou se podem ser adotados outros referenciais ou medidas equivalentes.	Acolhido	Redação do artigo 23º alterada.

Artigo 24º-O n.º 3 do artigo 24.º prevê a possibilidade de adoção de normas complementares ao QNRCS por autoridades setoriais, mas não aborda a eventual certificação do próprio QNRCS enquanto referencial nacional.	Não acolhido	O artigo 27.º do presente Regulamento já dispõe sobre a certificação do QNRCS.
Artigo 26º- Aplicação conjunta- Redundância da aplicação do QNRCS	Considerado	Redação do artigo 26º alterada.
Artigo 27º- Certificação voluntária- Limites de presunção de cumprimento das medidas de cibersegurança e clarificação do nº5 do artigo 27º	Parcialmente acolhido	Redação do artigo 27.º clarificada.
Artigo 28º- O n.º 5 do artigo 28.º prevê apenas de forma facultativa ("pode") a disponibilização, pelo CNCS, de um quadro de apoio à leitura da matriz de risco, não assegurando um nível mínimo de suporte às entidades na aplicação deste instrumento crítico.	Considerado.	Redação do artigo 28º clarificada.
Artigo 30º- Medidas de Cibersegurança Mínimas - Critérios de verificação e medidas equivalentes	Não acolhido	O disposto no artigo 27º do Regulamento já prevê a possibilidade de uma presunção de cumprimento de medidas cibersegurança previstas nos artigos 26º a 29º do Decreto-Lei n.º 125/2025 e 30º do Regulamento, através dos esquemas de certificação elencados no nº3 do artigo 27º do Regulamento.

Artigo 31º- O n.º 2 do artigo 31.º estabelece a obrigação de revisão das medidas de cibersegurança, mas não define uma periodicidade mínima nem clarifica os pressupostos que determinam a necessidade dessa revisão.	Acolhido	Redação do artigo 31º alterada.
Artigo 32º- A criação de uma lista centralizada de ativos publicamente acessíveis envolve informação sensível do ponto de vista da segurança, podendo aumentar a superfície de ataque caso seja excessivamente detalhada ou não estejam claramente definidas as respetivas finalidades e medidas de proteção, contrariando os princípios de segurança por defeito.	Parcialmente acolhido	A lista de ativos é essencial para o zelo eficaz e pleno de uma cultura robusta de cibersegurança no contexto nacional, e a sua exigência não é prejudicial às entidades. Redação do artigo 5.º alterada quanto à natureza classificada da informação.
Básico GR.CO-3- Clarificar a evidência mínima aceite ao nível Básico	Não acolhido	Os critérios de verificação dos anexo III e IV são evidências factuais, documentais ou técnicas consideradas adequadas pelas autoridades de cibersegurança competentes para evidenciar a implementação das medidas de cibersegurança. No entanto cabe a cada entidade definir a forma de implementação da medida de cibersegurança, cabendo às autoridades de cibersegurança competentes em sede de supervisão avaliar adequada implementação das medidas e o respetivo cumprimento do Regime Jurídico da Cibersegurança.
Básico GR.CO-4 / GR.CO-6- Recomenda-se que não seja exigida a comunicação dos serviços críticos, limitando-se a obrigação à respetiva identificação e gestão	Parcialmente acolhido	GR.CO-4- Redação alterada GR.CO-6 A medida apenas refere que a comunicação deve ser feita às partes interessadas, não explícita às partes interessadas externas.

interna, em função do risco, sem imposição de divulgação ou comunicação a partes interessadas.		
Básico GR.FR-4- Recomenda-se a clarificação orientadora do alcance da cibersegurança nos processos de gestão de recursos humanos, designadamente quanto à política de uso aceitável, de modo a evitar interpretações divergentes quanto ao seu alcance e grau de formalização exigidos.	Acolhido	Redação Alterada
Básico- GR.PP-1- Recomenda-se clarificar que as políticas de cibersegurança, enquanto documentos estratégicos e de alto nível, não têm de detalhar responsabilidades operacionais, as quais podem constar de documentação complementar, como procedimentos ou modelos de governação.	Não acolhido	Regulamento define as medidas mínimas de cibersegurança obrigatórias aplicáveis de forma abrangente, transversal e pretendendo abarcar o maior número de situações. A verificação da aplicação das medidas tem em conta o princípio da proporcionalidade.
Básico GR.CA -7- Recomenda-se a clarificação do conceito de ambiente operacional.	Parcialmente acolhido	Redação alterada. O CNCS irá emitir orientações complementares quanto à implementação dos controlos.
Básico ID.GA-5- Recomenda-se a clarificação do conceito de "tempo" no âmbito da gestão de ativos, designadamente quanto ao seu significado e aplicação prática.	Acolhido	Redação alterada
Básico PR.GA-3-A exigência genérica de autenticação multifator (MFA) para todos os ativos pode revelar-se excessiva e	Acolhido	Redação alterada

desproporcionada, sobretudo no nível Básico, ao não distinguir entre diferentes perfis de risco, tipos de acesso ou criticidade dos sistemas.		
Básico PR.FC-2- Recomenda-se clarificar que o controlo PR.FC-2 se aplica ao pessoal com funções técnicas ou operacionais de cibersegurança, devendo a formação dos membros do órgão de administração assumir natureza distinta, adequada às suas funções de administração e supervisão.	Acolhido	Redação alterada
Básico DE.MC-1- Clarificar que, no nível Básico, é admissível a adoção de mecanismos de monitorização limitados, baseados em ferramentas standard de segurança ou em serviços externalizados simples, desde que adequados ao nível de risco identificado e suficientes para a deteção de eventos relevantes de cibersegurança.	Não acolhido	Os critérios de verificação dos anexo III e IV são evidências factuais, documentais ou técnicas consideradas adequadas pelas autoridades de cibersegurança competentes para evidenciar a implementação das medidas de cibersegurança. No entanto cabe a cada entidade definir a forma de implementação da medida de cibersegurança, cabendo às autoridades de cibersegurança competentes em sede de supervisão avaliar adequada implementação das medidas e o respetivo cumprimento do Regime Jurídico da Cibersegurança.
Básico DE.AE-6- Referenciar explicitamente, no Regulamento ou em orientações técnicas complementares revistas e atualizadas, as taxonomias e critérios adotados pelo CNCS e pelo CERT.PT como orientação para a classificação de incidentes, promovendo uma interpretação uniforme e reduzindo o risco de divergências na qualificação das ocorrências.	Não acolhido	Não acolhido, extravasa o âmbito do Regulamento.

Substancial GR.CO-6- Recomenda-se clarificar que o controlo GR.CO-6 exige apenas a identificação dos serviços externos dos quais a entidade depende, sem impor a sua comunicação, assegurando a proporcionalidade do controlo e a minimização da partilha de informação sensível.	Acolhido	Redação alterada no Nível Básico.
Substancial GR.GR-1- Controlo alinhado com ISO 27001/31000. A exigência de formalização é pertinente neste nível.	Não acolhido	O Regulamento define as medidas mínimas de cibersegurança obrigatórias aplicáveis de forma abrangente, transversal e pretendendo abarcar o maior número de situações. A verificação da aplicação das medidas tem em conta o princípio da proporcionalidade.
Substancial GR.GR-5- Clarificar explicitamente que a política de gestão de riscos de cibersegurança pode estar integrada na política global de gestão de risco da entidade, desde que esta abranja de forma adequada os riscos de cibersegurança, evitando duplicações documentais e promovendo uma abordagem integrada e eficiente à gestão do risco.	Não acolhido	O Regulamento define as medidas mínimas de cibersegurança obrigatórias aplicáveis de forma abrangente, transversal e pretendendo abarcar o maior número de situações. A verificação da aplicação das medidas tem em conta o princípio da proporcionalidade.
Substancial GR.PP-1- No controlo GR.PP-1, existe falta de alinhamento entre o âmbito do controlo, que se refere a políticas de gestão da cibersegurança, e as evidências indicadas, que remetem para uma política específica (Política de Classificação e Gestão de Dados).	Não acolhido	O título do controlo é mais genérico e é abrangente o suficiente para ser aplicado por todas as entidades. Pelo contrário, as medidas mínimas de cibersegurança densificam o controlo, criando uma obrigatoriedade de aplicação que poderá revelar-se ou não mais restrita do que o próprio controlo.
Substancial GR.CA-7- No âmbito do controlo GR.CA-7, e de acordo com o nível de conformidade aplicável	Parcialmente acolhido	Redação alterada. O CNCS irá emitir orientações complementares quanto à implementação dos controlos.

(Básico, Substancial ou Elevado), reconhecer explicitamente, no Regulamento ou em orientações complementares, a utilização de modelos de avaliação contínua do risco e da cibersegurança da cadeia de abastecimento, admitindo métodos reconhecidos no mercado que assegurem monitorização regular, mecanismos de reporte adequados e integração na governação corporativa, evitando a imposição de modelos paralelos ou redundantes.		
Substancial ID.GA-6- Recomenda-se clarificar expressamente o conceito de metadados no âmbito do controlo ID.GA-6.	Acolhido	Redação alterada.
Substancial ID.AR-7- Indique onde está definida e acessível a Política Nacional de Divulgação Coordenada de Vulnerabilidades.	Considerado	O CNCS irá emitir uma instrução técnica da Divulgação Coordenada de Vulnerabilidades.
Substancial- RS.GI- Reconhecer explicitamente a realização de exercícios de simulação e o tratamento de incidentes reais como evidência suficiente de cumprimento dos controlos aplicáveis, evitando a exigência de documentação adicional redundante quando a eficácia operacional das medidas se encontre devidamente demonstrada.	Não acolhido	Os critérios de verificação dos anexo III e IV são evidências factuais, documentais ou técnicas consideradas adequadas pelas autoridades de cibersegurança competentes para evidenciar a implementação das medidas de cibersegurança. No entanto cabe a cada entidade definir a forma de implementação da medida de cibersegurança, cabendo às autoridades de cibersegurança competentes em sede de supervisão avaliar adequada implementação das medidas e o respetivo cumprimento do Regime Jurídico da Cibersegurança.
Substancial RS.NC-1- Clarificar que a comunicação de incidentes às partes interessadas	Não acolhido	Regulamento define as medidas mínimas de cibersegurança obrigatórias aplicáveis de forma abrangente, transversal e pretendendo abarcar o maior número de situações.

internas e externas é gerida pela própria entidade.		A verificação da aplicação das medidas tem em conta o princípio da proporcionalidade.
Substancial RC.CO-1- Clarificar que a comunicação das atividades de recuperação às partes interessadas internas e externas é gerida pela própria entidade, devendo ocorrer de forma coordenada e em conformidade com a legislação aplicável, designadamente em matéria de cibersegurança, proteção de dados pessoais e deveres de confidencialidade.	Não acolhido	Regulamento define as medidas mínimas de cibersegurança obrigatórias aplicáveis de forma abrangente, transversal e pretendendo abarcar o maior número de situações. A verificação da aplicação das medidas tem em conta o princípio da proporcionalidade.
Elevado- GR.FR-1- Clarificar, de forma objetiva, os tipos de evidência admissíveis para demonstrar o compromisso da gestão.	Não acolhido	Os critérios de verificação dos anexo III e IV são evidências factuais, documentais ou técnicas consideradas adequadas pelas autoridades de cibersegurança competentes para evidenciar a implementação das medidas de cibersegurança. No entanto cabe a cada entidade definir a forma de implementação da medida de cibersegurança, cabendo às autoridades de cibersegurança competentes em sede de supervisão avaliar adequada implementação das medidas e o respetivo cumprimento do Regime Jurídico da Cibersegurança.
Elevado- GR.SP-2- Controlo duplicado.	Acolhido	Redação alterada.
Elevado GR.CA-7- No âmbito do controlo GR.CA-7, e de acordo com o nível de conformidade aplicável (Básico, Substancial ou Elevado), reconhecer explicitamente, no Regulamento ou em orientações complementares, a utilização de modelos de avaliação contínua do risco e da cibersegurança da cadeia de abastecimento,	Parcialmente acolhido	Redação alterada. O CNCS irá emitir orientações complementares quanto à implementação dos controlos.

admitindo métodos reconhecidos no mercado que assegurem monitorização regular, mecanismos de reporte adequados e integração na governação corporativa, evitando a imposição de modelos paralelos ou redundantes.		
Elevado – ID.MC-2- Controlo duplicado.	Acolhido	Redação alterada.
Elevado-PR.GA-3- Recomenda-se a revisão da medida, uma vez que a mesma não se encontra devidamente alinhada com o controlo a que se associa.	Não acolhido	O título do controlo é mais genérico e é abrangente o suficiente para ser aplicado por todas as entidades. Pelo contrário, as medidas mínimas de cibersegurança densificam o controlo, criando uma obrigatoriedade de aplicação que poderá revelar-se ou não mais restrita do que o próprio controlo.
O.PSF - Política de Segurança de fornecedores- No âmbito da Política de Segurança de Fornecedores (O.PSF), e de acordo com o nível de conformidade aplicável (Básico, Substancial ou Elevado), recomenda-se o reconhecimento explícito, no Regulamento ou em orientações complementares, da utilização de modelos de avaliação contínua do risco e da cibersegurança da cadeia de abastecimento, admitindo métodos reconhecidos no mercado que assegurem monitorização regular, mecanismos de reporte adequados e integração na governação corporativa, evitando a imposição de modelos paralelos ou redundantes.	Parcialmente acolhido	Redação alterada. O CNCS irá emitir orientações complementares quanto à implementação dos controlos.
Outros comentários-	Acolhido	Redação alterada.

Na página 40, a identificação do controlo GR.PL-2 utiliza a sigla PL; contudo, atendendo à nomenclatura adotada na sequência dos controlos, cremos que a designação será GR.PP-2, garantindo coerência na taxonomia utilizada.		
APECYS		
Plataforma eletrónica, autoidentificação e registo	Não acolhido	A matéria do contributo já consta dos artigos 8.º e 10.º do Regulamento.
Cadeia de abastecimento e aplicação do princípio da proporcionalidade	Não acolhido	O artigo 28.º do Decreto-Lei n.º 125/2025 não carece de regulamentação.
Responsável de cibersegurança e ponto de contacto permanente	Não acolhido	Extravasa o âmbito do Regulamento.
Gestão do risco residual e lista de ativos publicamente acessíveis	Acolhido	Redação do artigo 31º clarificada e alterada para constar a análise e gestão do risco de cibersegurança e do risco residual. Redação do artigo 32º alterada.
Notificação de incidentes, instrumentos complementares e entrada em vigor	Acolhido	Norma de produção de efeitos alterada.
Entidades públicas relevantes e critérios de verificação	Não acolhido	Os critérios de verificação dos anexo III e IV são evidências factuais, documentais ou técnicas consideradas adequadas pelas autoridades de cibersegurança competentes para evidenciar a implementação das medidas de cibersegurança. No entanto cabe a cada entidade definir a forma de implementação da medida de cibersegurança, cabendo às autoridades de cibersegurança competentes em sede de supervisão avaliar adequada implementação das medidas e o respetivo cumprimento do Regime Jurídico da Cibersegurança. As medidas do Anexo IV são medidas aplicáveis a entidades de um âmbito muito específico, com uma exposição ao risco diferente. As medidas aplicadas às entidades públicas relevantes, presente no Anexo

		IV, são propositadamente distintas das medidas do quadro. No entanto, existem certas entidades públicas relevantes que, por serem qualificadas essenciais ou importantes, vão estar sujeitas às medidas do quadro.
Certificação, reconhecimento de esquemas e redução dos custos de contexto	Parcialmente acolhido	Redação alterada.
OEID		
Recomendações	Não acolhido	Os contributos não incidem sobre matéria concreta do Regulamento.
SONAE		
Artigo 6º- Criação de múltiplas contas	Acolhido	Redação do artigo 6º alterada.
Artigo 15º- Equipas Ponto de Contacto Permanente- Formulação da alínea a) do n.º 2 do artigo 15º parece impossibilitar a designação de uma equipa ou serviço como ponto de contacto permanente (por exemplo, um SOC externo com múltiplas equipas a assegurar um regime 24/7). Deveria	Acolhido	Redação do artigo 15º alterada.
Artigo 27º- Mapa equivalência certificações- Atendendo a que as certificações podem ter âmbitos diminutos face à amplitude dos ativos a contemplar em sede do Regime Jurídico de Cibersegurança, o âmbito das certificações deve ser alvo de escrutínio por parte do CNCS, garantindo que o mesmo inclui, no mínimo, a atividade/atividades que levou à qualificação da entidade como essencial	Considerado	Redação do artigo 27º clarificada.

ou importante. Tal obrigação de escrutínio deve estar formalizada no regulamento.		
Artigo 28º- Matriz de Risco- Assim, o n.º 4 deveria assegurar que são determinadas, de acordo com os cenários de riscos de cada setor, as medidas específicas do QNRCS e respetivo nível de conformidade para tratamento do cenário de risco.	Considerado	Redação do artigo 28º clarificada.
Artigo 30º- Medidas de Cibersegurança Mínimas- Certificação- O n.º 4 refere a possibilidade de exigência às entidades, por parte do CNCS, da obtenção de certificação em matéria de cibersegurança. No entanto, não são detalhadas as condições sob as quais o CNCS poderá proceder a tal exigência.	Não acolhido	Resulta da aplicação das regras gerais do Código do Procedimento Administrativo.
Artigo 31º- Gestão de risco residual- • "Risco residual", na aceção da literatura de referência (ISO 27005, NIST SP 800-30), define-se como a porção de risco remanescente após a implementação de medidas de segurança, não sendo o mesmo alvo de mais tratamento. O processo descrito neste artigo assume-se como uma nova iteração do processo de gestão de risco, pelo que o n.º 2 deveria referir-se a analise de risco e não a análise de risco residual, visto que é	Acolhido	Redação do artigo 31º alterada e clarificada.

esta nova iteração que levará ao cálculo do risco residual.		
Artigo 32º- Lista de Ativos-A alínea g) do n.º 2 requere a comunicação das "dependências entre os ativos, quando existentes", no entanto, não é detalhado no regulamento como devem ser especificadas as dependências, nem que tipos de dependências devem ser consideradas (nomeadamente processuais, tecnológicas ou contratuais).	Parcialmente acolhido	Redação do artigo 32º alterada.
Qualificação das entidades- • A definição de Produtores invocada no Regime Jurídico de Cibersegurança (artigo 2.º, ponto 38 da Diretiva (UE) 2019/944 – "uma pessoa singular ou coletiva que produz eletricidade"), coloca no âmbito dos setores de importância crítica as entidades com Unidades de Produção para Autoconsumo (UPAC).	Não acolhido	Extravasa o âmbito do Regulamento.
SPMS		
Artigo 6º, nº3- Acesso à área reservada- Sugere-se, assim, a previsão de registo técnico de acessos, ainda que em moldes proporcionais.	Não acolhido	O disposto no artigo 6º, nº3 refere-se ao acesso a conteúdo meramente informativo e não requer autenticação.
Artigo 6º, nº4- Perfis - Sugere-se a substituição de "ou" por "e/ou", ou outra formulação equivalente que assegure o acesso simultâneo ao responsável de cibersegurança e à(s) pessoa(s) que desempenha(m) a função	Não acolhido	Preocupação acautelada pelo elenco alternativo da norma.

de ponto de contacto permanente, no âmbito das respetivas competências.		
Artigo 17º, nº2- Confirmação da receção da notificação e comunicação de informação	Acolhido	Redação alterada.
Artigo 25º, nº 2- Estrutura QNRCS	Acolhido	Redação alterada.
Artigo 28º- Lacuna quanto à densificação da gestão de risco da cadeia de abastecimento.	Não acolhido	O artigo 28.º do Decreto-Lei n.º 125/2025 não carece de regulamentação.
Eversheds Sutherland- Contributo 2		
1-Prazo para elaboração do relatório anual	Não acolhido	Não é um contributo para efeitos de consulta pública.
2- Registo de entidades- Gamas de IP	Não acolhido	Não é um contributo para efeitos da consulta pública. Não obstante, a questão já está devidamente acautelada no artigo 10.º nº1 do Regulamento.
TAG		
Anexo III, Controlo GR.CA-7 (Avaliação do Risco da Cadeia de Abastecimento)	Parcialmente acolhido	Serão emitidas orientações complementares quanto aos controlos.
Matriz de Risco	Não acolhido	A Matriz de Risco não é alvo de consulta pública.
JCF		
Standardização de Evidências na Cadeia de Abastecimento (Anexo III –GR.CA-5 e GR.CA-7)	Não acolhido	Os critérios de verificação dos anexo III e IV são evidências factuais, documentais ou técnicas consideradas adequadas pelas autoridades de cibersegurança competentes para evidenciar a implementação das medidas de cibersegurança. No entanto cabe a cada entidade definir a forma de implementação da medida de cibersegurança, cabendo às autoridades de cibersegurança competentes em sede de supervisão avaliar adequada implementação das medidas e o respetivo cumprimento do Regime Jurídico da Cibersegurança.
Reconhecimento de Infraestrutura como Código (IaC) e GitOps	Não acolhido	Os critérios de verificação dos anexo III e IV são evidências factuais, documentais ou técnicas consideradas adequadas pelas autoridades de

(Anexo III – PR.SP-1 e ID.GA-9)		cibersegurança competentes para evidenciar a implementação das medidas de cibersegurança. No entanto cabe a cada entidade definir a forma de implementação da medida de cibersegurança, cabendo às autoridades de cibersegurança competentes em sede de supervisão avaliar adequada implementação das medidas e o respetivo cumprimento do Regime Jurídico da Cibersegurança.
Operacionalização dos Critérios de Declaração de Incidentes via SLIs (Anexo III – DE.AE-6)	Não acolhido	O Regulamento define as medidas mínimas de cibersegurança obrigatórias aplicáveis de forma abrangente, transversal e pretendendo abarcar o maior número de situações. A verificação da aplicação das medidas tem em conta o princípio da proporcionalidade.
Promoção de uma Cultura de Aprendizagem e Análises Pós-Incidente sem Culpa (Anexo III – ID.MC-3)	Parcialmente acolhido	Serão emitidas orientações complementares quanto aos controlos.
Follow(*)		
Relatório Anual das Entidades Públicas Relevantes	Não acolhido	Não configuram contributos para o Projeto de Regulamento.
Incongruência formal no Anexo II	Acolhido	Redação alterada.
Possível gralha de codificação no Anexo III	Acolhido	Redação alterada.
Incongruência de codificação no anexo III	Acolhido	Redação alterada.
Articulação entre os Anexos III e IV	Não acolhido	Não configuram contributos para o Projeto de Regulamento. As medidas do Anexo IV são distintas das medidas do Anexo III, originando de um documento distinto do Quadro Nacional de Referência para a Cibersegurança (QNRCS). A aplicação das medidas do Anexo IV será de aplicação obrigatória para as entidades públicas relevantes. As medidas do Anexo III serão de

		aplicação obrigatória para as entidades importantes e essenciais.
ActiveSys		
Quadro resumo de Objetivos e Categorias	Não acolhido	Não configuram contributos para o Projeto de Regulamento, porém, será disponibilizado pelo CNCS um quadro resumo do Quadro Nacional de Referência para a Cibersegurança (QNRCS).
Anexo III	Acolhido	Redação alterada.
O Anexo IV / grupo B	Não acolhido	As entidades públicas relevantes não têm a obrigação de comunicar o Responsável de Cibersegurança nem o Ponto de Contacto Permanente, nos termos do disposto no Decreto-Lei n.º 125/2025.
SMAS Torres Vedras		
Anexo III- Neste contexto, sugere-se que seja ponderada a inclusão, em anexo autónomo ou em alternativa ao atual Anexo III, de uma tabela de correspondência consolidada entre: a) todos os controlos do QNRCS (Anexo I); b) os respetivos níveis de conformidade aplicáveis; e c) as medidas e os critérios de verificação correspondentes.	Não acolhido	Não configuram contributos para o Projeto de Regulamento, porém, será disponibilizado pelo CNCS um quadro resumo do Quadro Nacional de Referência para a Cibersegurança (QNRCS).
Repetições dentro do mesmo nível de conformidade	Acolhido	Redação alterada.
Erro de codificação	Acolhido	Redação alterada.
Propostas de enquadramento de controlos atualmente sem nível atribuído	Não acolhido	Os controlos de cibersegurança do Quadro Nacional de Referência para a Cibersegurança (QNRCS) pretendem ser abrangentes, enquanto as medidas de cibersegurança densificam e criam obrigações para as entidades, nesse sentido, por serem medidas mínimas de cibersegurança, considerou-se que certos controlos não exigiriam medidas.
Universidade do Algarve		

Artigo 14º- Responsável de cibersegurança- Entidades Públicas Relevantes	Não acolhido	Extravasa o âmbito da consulta pública.
Empresa de Seguros (não identificada)		
Contributos	Não acolhido	Extravasa o âmbito da consulta pública.
Faculdade de Ciências da Faculdade de Lisboa		
Conceito de risco- A definição de risco presente no Projeto de Regulamento do Regime Jurídico de Cibersegurança, importada do DL n.º 125/2025, a saber: "Medida da possibilidade de uma perda ou perturbação causada por um incidente, resultante da combinação da magnitude de tal perda ou perturbação e da probabilidade de ocorrência do incidente." não reflete o conceito de risco internacionalmente estabelecido. A redação refere-se a uma possibilidade, conceito relacionado à probabilidade, e não a um desvio dos objetivos. Propõe-se rever esta definição, a fim de corrigi-la e alinhá-la às definições já estabelecidas. Mais concretamente, propõe-se uma tradução correta da definição da Diretiva (EU) 2022/2555: "potencial de perda ou interrupção causado por um incidente, que deve ser expresso como uma combinação da magnitude dessa perda ou interrupção e da probabilidade de ocorrência do incidente."	Não acolhido	Extravasa o âmbito da consulta pública.

Parecer sobre incidente de impacto significativo- Importa definir claramente o que se entende por incidente de impacto significativo, no artigo 20.º: apresentar os limiares a considerar para os critérios elencados no artigo 40.º do DL n.º 125/2025 ou remeter ao disposto no Regulamento de Execução (UE) 2024/2690, de 17 de outubro de 2024.	Não acolhido	Será âmbito de instrução técnica nos termos no nº4 do artigo 40º.
APDC		
Clarificação do carácter vinculativo das disposições. Artigos 24.º e 27.º.	Acolhido	Redações alteradas em conformidade.
Articulação entre regimes e autoridades- A APDC identifica, de forma consistente, a necessidade de assegurar uma articulação clara e explícita entre o RJC e respetivo Regulamento e os regimes setoriais vigentes, em particular no domínio das comunicações eletrónicas (nomeadamente o Regulamento ANACOM n.º 303/2019), bem como com outros enquadramentos aplicáveis em matéria de notificação de incidentes, incluindo o RGPD e demais legislação relevante.	Não acolhido	Ultrapassa o âmbito material do Regulamento.
Proporcionalidade e segurança jurídica na certificação e auditorias	Não acolhido	Resulta do âmbito do Código do Procedimento Administrativo.
Artigo 1º e Anexos I, II e III- Não resulta claro se os critérios de verificação do Anexo III e as medidas de cibersegurança mínimas são obrigatórios para entidades essenciais e importantes, ou	Parcialmente acolhido	Redação do artigo 1º alterada.

meramente recomendados.		
Artigo 4º - Funcionalidade da Plataforma- funções e responsabilidades- O artigo não contempla disposições sobre funções e responsabilidades associadas à plataforma, nem sobre delegação de competências (o que delegar e em quem se pode delegar).	Parcialmente acolhido	Redação do artigo 4º alterada. A fixação de prazo de 180 dias extravasa o âmbito do regulamento.
Artigo 6º - Acesso à plataforma com os diversos perfis- Não é claro como deve funcionar o acesso em grupos empresariais com várias empresas abrangidas pelo RJC (ex. CISO de grupo), nem se é possível um registo único para o grupo.	Acolhido	Redação do artigo 6º alterada.
Artigo 8º - Registo por entidade ou registo por setor- Não resulta claro se uma entidade que presta múltiplos serviços abrangidos pelo RJC deve efetuar um registo único (identificando todos os serviços) ou um registo autónomo por serviço.	Acolhido	Redação do artigo 8º alterada.
Artigo 9º- A responsabilidade pela qualificação não está suficientemente articulada com as autoridades setoriais competentes, em particular a ANACOM.	Não acolhido.	Resulta do Decreto-Lei n.º 125/2025 que a responsabilidade da qualificação cabe ao CNCS.
Artigos 12º, 14º, 15º- Art. 12.º: Não é claro se todas as comunicações (incluindo Relatório Anual ou Inventário de Ativos) têm um valor a pagar, nem quem suporta o custo. Art. 14.º/15.º: Inconsistência de prazos — os artigos 31.º e 32.º do RJC impõem a comunicação do	Parcialmente Acolhido	Redação dos artigos 14º e 15º alterada. Não haverá lugar a pagamento quanto às comunicações.

Responsável de Segurança e do Ponto de Contacto até 4 de maio, prazo que não está articulado com os 60 dias para autoidentificação na plataforma, levando a comunicar responsáveis antes de concluir a autoidentificação.		
Art. 17.º: Não consta o endereço eletrónico para notificação em situações de falência do sistema.	Considerado	O endereço eletrónico deverá ser indicado em instrumento externo ao Regulamento, para permitir a sua atualização.
Artigos 20º e 21º- Notificação de Incidentes- O modelo de notificação faseado (notificação inicial, notificação de fim de impacto, relatório intercalar e relatório final) não assegura articulação expressa com outros regimes de notificação (RGPD, comunicações eletrónicas, CNPD).	Não acolhido	Extravasa o âmbito da consulta pública.
Artigos 23º e 26º- O artigo 24.º não esclarece se a adoção do QNRCS é obrigatória para entidades essenciais e importantes.	Acolhido	Redação dos artigo 23º e 26º alterada
Artigo 27º certificação voluntária- A certificação voluntária não prevê qualquer dispensa ou suavização dos requisitos de auditorias periódicas (artigo 54.º), o que desincentiva a certificação e gera sobreposição de obrigações. A multiplicidade de auditorias (NIS2, certificação, auditoria interna) cria sobrecarga administrativa e custos desnecessários. O âmbito de validade das certificações (ex. ISO 27001) não é clarificado.	Parcialmente acolhido	Redação alterada quanto à ISO 27001. Quanto aos atos de supervisão, o contributo extravasa o âmbito do Regulamento.

Artigo 28º Matriz de Risco- Densificar os critérios de classificação de risco no regulamento, incluindo métricas quantitativas e qualitativas. Prever um procedimento formal com: notificação da classificação atribuída e respetiva fundamentação; direito de pronúncia prévia; mecanismo claro de revisão ou impugnação. O CNCS deve disponibilizar a matriz de risco para análise e esclarecimento pelas entidades abrangidas.	Parcialmente acolhido	Redação do artigo 28º clarificada. O procedimento de qualificação foi densificado para permitir a pronúncia prévia à decisão.
Artigos 30º e 31º - Certificações impostas e Risco Residual- Art. 30.º, n.º 4: Confere ao CNCS poderes para exigir certificações sem critérios materiais, condições procedimentais ou exigências de fundamentação, gerando grau elevado de discricionariedade. Art. 31.º: Não densifica metodologias mínimas de identificação, avaliação e tratamento do risco, nem critérios de aceitação do risco residual. A ligação ao Regulamento de Execução (UE) 2024/2690 não está clarificada no n.º 5.	Parcialmente acolhido	Redação do artigo 30.º e 31º alteradas.
Artigo 33º - Medidas de Execução- Não é claro se as medidas de execução previstas no n.º 1 são aplicáveis a clientes residenciais no setor das telecomunicações.	Não acolhido	Os artigos 56.º e 57.º do Decreto-Lei nº 125/2025 apenas dizem respeito às entidades essenciais, importantes e públicas relevantes.
FASTFIBER		
Aditamento ao artigo 1.º e possível violação do princípio da proporcionalidade	Não acolhido	Os princípios referidos no contributo já resultam do próprio Decreto-Lei nº 125/2025.

Densificação do conceito de incidente significativo – falta de conceito operativo central.	Não acolhido	A matéria a que respeita o contributo será alvo de instrução técnica, nos termos no nº4 do artigo 40º do Decreto-Lei nº 125/2025.
Reforço do papel da plataforma enquanto instrumento único de comunicação. Proposta de alteração aos artigos 4.º e 5.º.	Considerado	O Regulamento já prevê, no nº 4 do seu artigo 4.º, a interoperabilidade nas comunicações das entidades, realizadas através da plataforma eletrónica, no que toca à notificação de incidentes significativos. O artigo 12º dispõe quanto à comunicação das entidades através da plataforma eletrónica com a autoridade de cibersegurança competente. Não obstante, o contributo é pertinente e foi tido em conta.
Minimização da recolha de dados na autoidentificação (artigo 8.º)	Não acolhido	O artigo 8.º já prevê, de forma expressa no 1.º, a recolha dos dados estritamente necessários à qualificação das entidades.
Reforço do dever de fundamentação das decisões no artigo 9.º. Proposta de alteração da redação.	Não acolhido	Os deveres de fundamentação resultam do regime geral do Código do Procedimento Administrativo, pelo que a matéria não carece de regulamentação.
Clarificação da contagem dos prazos para as notificações de incidentes significativos. Proposta de alteração da redação do artigo 20.º.	Não acolhido	Os prazos para o reporte de incidentes significativos, bem como a sua contagem, estão definidos no Decreto-Lei nº 125/2025 e não pode o Regulamento derrogá-los. Não obstante, a qualidade da informação reportada é assegurada pela existência do mecanismo de atualização de reporte da notificação inicial, nos termos do nº3 do artigo 42.º do Decreto-Lei nº 125/2025.
Consagração do princípio da proporcionalidade nas medidas de segurança. Proposta de alteração do artigo 30.º.	Considerado	O Regulamento define as medidas mínimas de cibersegurança obrigatórias aplicáveis de forma abrangente, transversal e pretendendo abarcar o maior número de situações. A verificação da aplicação das medidas tem em conta o princípio da proporcionalidade, bem como o perfil de risco e a dimensão da entidade. Não obstante, redação do artigo 30.º foi clarificada.
Clarificação do alcance da obrigação de comunicação da lista de ativos.	Considerado	A realização do inventário de ativos pelas entidades é exigida nas medidas mínimas de cibersegurança. Nesse sentido, a lista de ativos do artigo 32º

		do Regulamento terá por base o inventário de ativos já exigido em sede de medidas mínimas. Da lista de ativos apenas constam os ativos diretamente acessíveis publicamente através da Internet. Não obstante, redação do artigo 32.º clarificada.
Garantia do contraditório e proporcionalidade nas medidas de execução. Proposta de alteração do artigo 33.º	Não acolhido	O artigo 53.º do Decreto-Lei nº 125/2025, para o qual o artigo 33.º do Regulamento remete expressamente, já prevê o disposto no contributo.
INCM		
A redação do artigo 1.º do Projeto de Regulamento apresenta-se excessivamente genérica, limitando-se a indicar que o diploma procede à regulamentação de diversas matérias previstas no Regime Jurídico da Cibersegurança (RJSC).	Considerado	O artigo 1º assegura os objetivos propostos.
O artigo 2.º do Projeto de Regulamento define o respetivo âmbito de aplicação subjetivo	Não acolhido	Os vários artigos do Regulamento dispõem quanto ao âmbito de aplicação, quanto à qualificação das entidades.
Melhoria e maior clareza das definições do artigo 3º	Parcialmente acolhido	Redação do artigo 3º alterada.
Centralização das funções na Plataforma e garantias mínimas para as entidades-artigo 4º.	Considerado	O contributo não carece de previsão no presente Regulamento.
A redação atual do artigo 5º centra-se na obrigação de disponibilização da plataforma, pressupondo a sua existência, acessibilidade e funcionalidade, mas não explicita os parâmetros jurídicos mínimos associados a essa disponibilização.	Considerado	A matéria do contributo resulta já das normas do CPA, nomeadamente o seu nº2 do artigo 14.º.
A redação atual do artigo 6º apresenta uma listagem ampla de finalidades, mas fá-lo numa lógica predominantemente descritiva, sem clarificar suficientemente o alcance	Considerado	Redação do artigo 6º clarificada.

jurídico dessa centralização funcional.		
Artigo 7º- Sem questionar os mecanismos de autenticação adotados, justifica-se clarificar a separação entre autenticação e representação jurídica, bem como o regime de imputação.	Considerado	Redação do artigo 7º clarificada.
Artigo 8º- A opção por um modelo de autoidentificação declarativa é funcionalmente compreensível, mas a redação atual do artigo não densifica suficientemente o estatuto jurídico dessa declaração, nem as consequências de eventuais erros ou divergências de interpretação.	Considerado	Redação do artigo 8º clarificada.
A redação atual do artigo 9º centra-se no poder da autoridade competente para proceder à qualificação, mas não densifica suficientemente o respetivo procedimento, nem as garantias associadas à posição da entidade.	Considerado	Redação do artigo 9º clarificada.
A redação atual do artigo 10º centra-se na lógica funcional de registo, mas não clarifica de forma suficientemente explícita os efeitos jurídicos associados ao registo definitivo, nem a articulação com situações de atraso, pendência ou divergência.	Não considerado	O artigo 10º já define expressamente o funcionamento da Plataforma e quanto aos efeitos jurídicos do registo definitivo, quando lido em conjunto com o disposto no artigo 3º. Adicionalmente, a consolidação do registo provisório em definitivo depende da notificação de qualificação das entidades.
Apesar da sua importância estrutural, a redação atual do artigo 11º é ampla e genérica, não densificando de forma suficiente o conteúdo, alcance e limites	Não acolhido	A atualização da informação na Plataforma eletrónica decorre do disposto no nº1 do artigo 8º do Decreto-Lei n. º 125/2025.

jurídicos do dever de atualização.		
A redação atual do artigo 12º adota uma formulação ampla, centrada no meio privilegiado de comunicação, mas não densifica suficientemente o estatuto jurídico dessas comunicações, nem distingue as respetivas categorias.	Considerado	Redação do artigo 12º clarificada.
A redação atual do artigo 13º privilegia uma lógica funcional de submissão eletrónica, mas não densifica suficientemente o estatuto jurídico dos documentos comunicados, nem regula aspetos essenciais como autoria, integridade, atualidade ou valor probatório.	Não acolhido	O artigo 13º densifica o envio do Relatório Anual via Plataforma eletrónica, envio esse que decorre de uma obrigação prevista no artigo 30º do Decreto-Lei n.º 125/2025. O artigo dispõe ainda quanto aos documentos a serem enviados, se necessário, do que resulte das medidas de cibersegurança ou dos exercícios de poderes de supervisão, que são documentos que resultam do cumprimento de obrigações.
A redação atual do artigo 14º identifica corretamente a necessidade de designação de um responsável, mas não densifica de forma suficiente o estatuto jurídico e funcional da função, nem clarifica a sua articulação com outros papéis internos já existentes nas organizações.	Não acolhido	O contributo reflete matérias que extravasam o âmbito do Regulamento, nomeadamente quanto à acumulação de funções, uma vez que as obrigações do Responsável de Cibersegurança se encontram dispostas no artigo 31º do Decreto-Lei n.º 125/2025.
A redação atual do artigo 15º consagra corretamente a necessidade de um ponto de contacto permanente, mas não densifica suficientemente o seu alcance funcional, nem a sua articulação com a figura do responsável de cibersegurança.	Não acolhido	O contributo reflete matérias que extravasam o âmbito do Regulamento, uma vez que as obrigações do Ponto de Contacto Permanente se encontram dispostas no artigo 32º do Decreto-Lei n.º 125/2025.
A redação atual do artigo 16º adota uma abordagem funcional, mas não densifica suficientemente	Não acolhido	O artigo 16º dispõe quanto ao tratamento dos dados pessoais no âmbito do Regime Jurídico da Cibersegurança, definindo quais os

os princípios materiais aplicáveis ao ciclo de vida dos dados, nem clarifica os limites do tratamento em função das finalidades.		prazos de conservação dos mesmos. O artigo deve ser lido em conjunto com o disposto no artigo 11º do Regulamento.
A inclusão desta norma (artigo 17º) é positiva e juridicamente necessária; contudo, a redação atual é sucinta e não densifica de forma suficiente o regime jurídico aplicável em cenários de falência, especialmente quanto aos efeitos, procedimentos alternativos e repartição de responsabilidades.	Acolhido	Redação do artigo 17º alterada.
A redação atual do artigo 18º reflete uma intenção positiva de eficiência administrativa, mas não densifica suficientemente os pressupostos, limites e garantias associados à interoperabilidade e ao acesso à informação.	Não acolhido	A matéria do contributo resulta já das normas do CPA, nomeadamente o seu artigo 14.º.
A redação atual do artigo 19º opta por uma solução funcional e coerente com a administração eletrónica, mas não densifica suficientemente o regime jurídico da notificação, nomeadamente no que respeita à presunção de conhecimento, à produção de efeitos e à tutela da confiança.	Considerado	Redação do artigo 19º alterada.
O artigo 20º densifica o regime previsto no Regime Jurídico da Cibersegurança, definindo o "como" e o "quando" da notificação, mas fá-lo sobretudo numa lógica funcional e operacional, deixando pouco densificado o enquadramento jurídico-garantístico da obrigação.	Não acolhido.	A notificação de incidentes decorre do disposto no Decreto-Lei n.º 125/2025. Os contributos extravasam o âmbito do Regulamento.

A redação atual do artigo 21º é sucinta e não densifica suficientemente o estatuto jurídico da notificação voluntária, o que pode comprometer a sua efetividade prática.	Não acolhido.	A notificação voluntária decorre do disposto no Decreto-Lei n.º 125/2025. Os contributos extravasam o âmbito do Regulamento.
A redação atual do artigo 22º centra-se na lógica funcional de acompanhamento do incidente, mas não densifica suficientemente o regime procedimental, nem estabelece de forma clara os direitos e deveres das entidades durante essa tramitação.	Parcialmente considerado.	Redação do artigo 22º alterada.
A redação atual do artigo 23º atribui ao QNRCS um relevo muito significativo, mas não densifica suficientemente o seu estatuto jurídico, nem clarifica os limites da sua força normativa.	Considerado	Redação do artigo 23º clarificada.
A redação atual do artigo 24º remete, em larga medida, para as categorias definidas no RJSC (entidades essenciais, entidades importantes e entidades públicas relevantes), mas não clarifica plenamente a lógica de distribuição das obrigações técnicas nem a eventual diferenciação do seu grau de aplicabilidade.	Não acolhido.	O conteúdo do contributo já se encontra devidamente densificado no Decreto-Lei nº. 125/2025 e no Regulamento, sendo que os artigos 23º ao artigo 26º foram clarificados.
A redação atual do artigo 25º descreve a estrutura do QNRCS de forma sistemática, mas não clarifica suficientemente o estatuto jurídico dos seus elementos internos, nem o grau de obrigatoriedade associado a cada nível da estrutura.	Considerado	Alterações efetuadas nos artigos 23º a 26º para refletir os contributos. Adicionalmente, no Anexo I do Regulamento encontram-se densificados alguns dos elementos do contributo.
A redação atual do artigo 26º limita-se a afirmar a	Considerado	Redação do artigo 26º clarificada.

aplicação conjunta, sem densificar os seus efeitos jurídicos concretos, nem esclarecer como devem ser resolvidas tensões ou sobreposições entre instrumentos.		
A redação atual do artigo 27º assume corretamente o caráter voluntário da certificação, mas não clarifica suficientemente os efeitos jurídicos associados à sua adoção, nem o seu peso efetivo no contexto do Regulamento.	Considerado	Redação do artigo 27º clarificada.
A redação atual do artigo 28º remete para a Matriz de Risco constante de anexo, conferindo-lhe uma função estruturante, mas não densifica suficientemente o seu estatuto jurídico-operativo, nem o modo como deve ser aplicada na prática.	Não acolhido.	A função da Matriz de Risco decorre do disposto no Decreto-Lei n.º 125/2025, sendo que o Regulamento densifica a sua aplicação.
A redação atual do artigo 29º retoma, em termos gerais, as categorias previstas no Regime Jurídico da Cibersegurança (entidades essenciais, entidades importantes e entidades públicas relevantes), mas fá-lo de forma pouco diferenciada, sem explicitar de modo claro como e em que medida a Matriz de Risco se aplica a cada uma dessas categorias.	Considerado.	Redação do artigo 29º totalmente alterada.
Apesar da sua centralidade, a redação atual do artigo 30º limita-se essencialmente a remeter para o anexo, sem densificar o estatuto jurídico das medidas mínimas, nem clarificar o seu papel face à lógica de	Parcialmente acolhido.	Redação do artigo 30º alterada.

proporcionalidade baseada no risco.		
A previsão da gestão do risco residual no artigo 31º é, em si mesma, positiva e necessária. Contudo, a redação atual do artigo não densifica suficientemente o seu regime jurídico, nem clarifica os efeitos da aceitação do risco residual em sede de supervisão e responsabilidade.	Considerado.	Redação do artigo 31º clarificada.
A introdução desta obrigação do artigo 32º é coerente com boas práticas internacionais de cibersegurança. Todavia, a redação atual do artigo não densifica suficientemente o alcance, o detalhe e o estatuto jurídico da lista, nem clarifica a sua utilização pela autoridade competente.	Considerado.	Redação do artigo 32º clarificada.
A redação atual do artigo 33º enfatiza a necessidade de execução das medidas, mas não densifica suficientemente o conteúdo, o grau de formalização e os critérios de avaliação das medidas de execução, o que pode gerar incerteza prática significativa.	Não acolhido.	As medidas de execução decorrem do já disposto nos artigos 56º e 57º, tendo sido o artigo 33º clarificado.