Anexo IV do Regulamento n.º 756/2026

as medidas das entidades públicas relevantes, grupo a grupo

1 de outubro de 2026

O Regime Jurídico da Cibersegurança trata a administração pública à parte. Um organismo público que não seja qualificado como entidade essencial ou importante é uma entidade pública relevante: não recebe um nível de conformidade nem aplica o Anexo III, aplica as medidas do Anexo IV do Regulamento n.º 756/2026 do CNCS, conforme pertença ao Grupo A ou ao Grupo B. O Anexo IV cabe em cinco páginas do Diário da República, e esta nota lê-o medida a medida.

Quem está em cada grupo

Os grupos são definidos no Decreto-Lei n.º 125/2025, e não no Regulamento (RJC, art. 7.º). No **Grupo A** ficam os serviços da administração direta com 250 ou mais trabalhadores, os da administração indireta e autónoma com mais de 250, as entidades públicas empresariais acima dos limiares de PME, as entidades administrativas independentes, e ainda o Conselho Económico e Social, a Provedoria de Justiça, os serviços da Presidência da República, da Assembleia da República e dos tribunais, o CSM, o CSTAF e o CSMP. No **Grupo B** ficam os serviços da administração direta, indireta e autónoma com 75 a 249 trabalhadores, e as entidades públicas empresariais que sejam médias empresas.

O Banco de Portugal, a CMVM e a ASF estão fora do regime como entidades administrativas independentes (RJC, art. 3.º, n.º 3). Um organismo que caiba em mais de uma categoria fica na mais exigente (art. 9.º), e um organismo público cuja missão seja a infraestrutura de TIC, ou com uma integração digital particularmente elevada, pode ser qualificado como entidade essencial (art. 6.º, n.º 1), e nesse caso sai do Anexo IV para o Anexo III.

A janela de dois anos

O dever de aplicar as medidas do Anexo IV (RJC, art. 33.º) e a coima por não o fazer (art. 61.º, n.º 1, al. f)) só produzem efeitos 24 meses após a publicação da regulamentação do regime (DL, art. 10.º, n.º 2). Com o Regulamento n.º 756/2026 publicado a 22 de junho de 2026, essa data é **22 de junho de 2028**. A conta assume que o Regulamento é toda a regulamentação a que o artigo se refere, e o próprio Regulamento acrescenta que as disposições que dependem de instruções técnicas do CNCS só produzem efeitos quando estas forem publicadas (Reg., art. 35.º, n.º 2).

A janela não se aplica a tudo. O dever de registo (RJC, art. 35.º) e o dever de notificar qualquer incidente significativo (art. 40.º) também se aplicam às entidades públicas relevantes e não constam da lista de efeitos diferidos, por isso não esperam por 2028. Quando a janela fechar, o incumprimento das medidas é uma contraordenação muito grave: de 16.000 € a 4.000.000 € no Grupo A, e de 8.000 € a 350.000 € no Grupo B, para a pessoa coletiva (art. 61.º, n.º 2).

Morada
Rua Major João Luís de Moura
Piso 1, Esc. AE · 1685-253 Famões

Contacto
hello@deltacoders.com

Web
deltacoders.com

Grupo B: dezoito medidas

O Anexo IV organiza cada grupo num quadro com três colunas: a área, a medida e o critério de verificação. O critério é a coluna que interessa, porque diz o que um supervisor vai pedir para ver. Das dezoito medidas do Grupo B, oito pedem evidência técnica, e as outras dez pedem um documento, um registo ou um inventário.

Medida	O que pede	Critério de verificação
O.CRI Ponto de contacto para resposta a incidentes	Uma pessoa identificada, capaz de responder a solicitações externas e, se necessário, contactável fora do horário de expediente.	Evidência documental sobre o ponto de contacto.
O.IAC Inventariação dos ativos críticos	Os ativos críticos para a atividade principal e as dependências entre eles, num inventário atualizado com regularidade.	Inventário atualizado dos ativos críticos.
O.GAP Gestão de acessos e permissões	Cada acesso novo, alterado ou revogado passa por um pedido e uma aprovação.	Evidência da gestão dos pedidos e das aprovações.
O.GEC Gestão de equipamentos computacionais	A atribuição e a recolha dos equipamentos documentadas e atualizadas.	Registo documentado da atribuição e da recolha.
O.PSF Política de segurança de fornecedores	Os fornecedores com acesso a sistemas de informação inventariados, com os contactos para notificação de incidentes.	Evidência documental da lista de fornecedores.
T.GPT Gestão de sistemas, aplicações e postos de trabalho	Controlos de segurança aplicados nos sistemas, nas aplicações e nos postos de trabalho.	Evidência técnica da implementação desses controlos.
T.PPT Proteção de postos de trabalho	Antivírus instalado nos postos de trabalho e nos servidores.	Evidência técnica da instalação.
T.AR Acesso remoto à entidade	Acesso remoto por um mecanismo seguro (VPN ou VDI, por exemplo) e com segundo fator de autenticação.	Evidência técnica do mecanismo e do segundo fator.
T.PAS Perfil de administração segregado	Utilizadores distintos para o uso aplicacional e para a administração.	Evidência documentada da segregação das contas.

Medida	O que pede	Critério de verificação
T.AS Atualizações de segurança	As atualizações de segurança recomendadas pelos fabricantes aplicadas atempadamente aos sistemas operativos e ao software dos postos de trabalho e servidores.	Registo documentado das atualizações.
T.PEW Proteção de correio eletrónico e serviços web	As boas práticas de segurança no correio eletrónico e nas páginas de internet.	Evidência técnica da autenticação do correio eletrónico e de protocolos seguros e certificados digitais nas páginas.
T.CS Cópias de segurança	Cópias de segurança feitas, e utilizáveis quando for preciso.	Evidência técnica da execução das cópias.
T.RAR Recolha e armazenamento de registos	Os registos definidos por defeito ativos nos sistemas operativos, aplicações e outros dispositivos.	Evidência técnica da ativação.
T.PPL Proteção perimetral da infraestrutura lógica	A proteção perimetral da infraestrutura.	Evidência técnica das medidas de segurança lógica nos equipamentos.
T.PPF Proteção perimetral da infraestrutura física	A proteção física dos espaços que alojam infraestrutura crítica, como um centro de processamento de dados.	Evidência técnica das medidas de segurança física nesses espaços.
T.MA Mecanismos de autenticação	Uma política que garanta palavras-passe com a robustez adequada à operação.	Evidência da implementação da política nas plataformas.
H-PF Sensibilização e formação	Ações de sensibilização ou de formação em cibersegurança.	Registo documentado das ações.
H.FIC Fontes de informação e canais de comunicação	Consulta regular de fontes fidedignas sobre ameaças, e acesso a canais de comunicação sobre elas.	Evidência dos canais de pesquisa e de disseminação.

Grupo A: mais vinte e duas

O Grupo A não tem uma lista própria que substitua a do Grupo B: aplica as dezoito medidas do Grupo B e soma-lhes as vinte e duas do seu quadro (Reg., art. 30.º, n.º 3), quarenta ao todo. Cinco das vinte e duas são políticas com o mesmo critério, “aprovada e implementada”, e nove pedem evidência técnica.

Medida	O que pede	Critério de verificação
O.PSI Política de cibersegurança	Uma política que fixe o compromisso da entidade com a cibersegurança.	Política aprovada e implementada.
O.IAC Inventariação dos ativos	Todos os ativos, e não só os críticos, com as dependências entre eles, num inventário atualizado com regularidade.	Inventário completo e atualizado.
O.PAP Política de acessos e permissões	Uma política de gestão de acessos e permissões, definida e implementada.	Política aprovada e implementada.
O.GEC Gestão de equipamentos computacionais	Os dispositivos pessoais separados dos dispositivos corporativos.	Evidência técnica da segregação de redes.
O.PUA Política de utilização aceitável	Uma política para toda a entidade, dada a conhecer a todo o pessoal, com requisitos para a confidencialidade e a integridade dos ficheiros trocados com outras entidades.	Política aprovada e implementada.
O.PP Política de palavra-passe	Uma política de gestão das palavras-passe.	Política aprovada e implementada.
O.PCF Classificação da informação	Um processo com critérios ou níveis de sensibilidade para os dados.	Registo documentado da classificação.
O.GMO Gestão da mudança organizacional	Procedimentos de TIC para a entrada, a mudança de funções e a saída de pessoal, sincronizados com os recursos humanos.	Registo documentado dos procedimentos.
O.ID Funções ou atividades críticas	As funções críticas identificadas, com as suas dependências das TIC.	Registo das funções, dos ativos que as suportam e das dependências entre eles.

Medida	O que pede	Critério de verificação
O.PSF Política de segurança de fornecedores	Uma política com a avaliação de risco da cadeia de abastecimento e os critérios de aceitação.	Política aprovada e implementada.
T.PPT Proteção de postos de trabalho	Controlo de acesso aos postos de trabalho e cópias de segurança da sua informação.	Evidência técnica do controlo de acesso e das cópias.
T.PPT Perfil de trabalho nos dispositivos móveis	A informação corporativa acedida só através de um perfil de trabalho no dispositivo móvel.	Evidência técnica da configuração do perfil.
T.GP Gestão de palavras-passe	As palavras-passe dos acessos privilegiados guardadas numa solução de gestão de palavras-passe.	Evidência técnica da solução.
T.PAD Privilégios de acesso diferenciados	Acessos concedidos pela necessidade de conhecer e pelo menor privilégio, em conformidade com a política de acessos.	Registo dos acessos por perfil funcional.
T.AS Atualizações de segurança	As atualizações recomendadas pelos fabricantes, agora também nos equipamentos de hardware.	Registo documentado da atualização do hardware.
T.AM Autenticação multifator	Autenticação multifator ativa nas aplicações críticas.	Evidência técnica da autenticação multifator.
T.PEW Proteção de correio eletrónico e serviços web	As mesmas boas práticas, com critérios mais exigentes.	Evidência técnica da autenticação e validação do correio eletrónico, de protocolos seguros, de certificados digitais e dos cabeçalhos de segurança nas páginas.
T.CS Cópias de segurança	As cópias de segurança guardadas à parte do ambiente que protegem.	Evidência técnica da segregação do armazenamento.

Morada
Rua Major João Luís de Moura
Piso 1, Esc. AE · 1685-253 Famões

Contacto
hello@deltacoders.com

Web
deltacoders.com

Medida	O que pede	Critério de verificação
T.RAR Recolha e armazenamento de registos	Os logs dos sistemas operativos, aplicações e outros dispositivos salvaguardados.	Evidência técnica da recolha de logs.
T.SC Securização (hardening) de configurações	Práticas de segurança nas configurações do posto de trabalho, do sistema operativo e das principais aplicações.	Evidência técnica das boas práticas.
H.EC Exercícios de phishing	Exercícios periódicos que avaliem a preparação do pessoal.	Registo dos resultados, das conclusões e das iniciativas que deles resultam.
H-PF Plano de formação	Um plano de formação em cibersegurança, com os processos para o executar.	Registo documentado dos planos e das ações.

O código T.PPT aparece duas vezes no quadro do Grupo A, para a proteção dos postos de trabalho e para o perfil de trabalho nos dispositivos móveis. Está assim no texto publicado; ao citar uma destas medidas, convém juntar a área ao código.

O que muda do Grupo B para o Grupo A

Nove códigos aparecem nos dois quadros, e em quase todos o Grupo A sobe um degrau em vez de repetir o pedido. O inventário deixa de ser só dos ativos críticos e passa a ser de todos (O.IAC). A gestão de equipamentos passa do registo de quem tem o quê para a separação técnica entre dispositivos pessoais e corporativos (O.GEC). Os fornecedores deixam de ser uma lista de contactos e passam a ter uma política com avaliação de risco e critérios de aceitação (O.PSF). As cópias de segurança, além de existirem, têm de ficar guardadas à parte do ambiente que protegem (T.CS). Os registos, além de ativos, têm de ser salvaguardados (T.RAR). As atualizações chegam ao hardware (T.AS), a proteção do correio e das páginas passa a incluir a validação do correio e os cabeçalhos de segurança (T.PEW), e a formação passa de ações avulsas a um plano (H-PF).

O resto do quadro do Grupo A é novo: as políticas de cibersegurança, de acessos, de utilização aceitável e de palavras-passe, a classificação da informação, as funções críticas, a mudança de pessoal articulada com os recursos humanos, a autenticação multifator nas aplicações críticas, o cofre de palavras-passe privilegiadas, o hardening e os exercícios de phishing.

Dois exemplos

Um instituto público com 120 trabalhadores. É administração indireta com 75 a 249 trabalhadores, portanto Grupo B, com dezoito medidas. A nossa leitura é que três delas vêm primeiro, porque as outras dependem delas ou porque o dever a que servem já está em vigor: o ponto de contacto para resposta a incidentes (O.CRI), porque a notificação de incidentes significativos já é obrigatória; o inventário dos ativos críticos (O.IAC), porque as medidas técnicas se aplicam a sistemas que é preciso conhecer primeiro; e a lista de fornecedores com acesso aos sistemas e os seus contactos para incidentes (O.PSF), porque um incidente num fornecedor é muitas vezes o primeiro que a entidade tem de notificar.

Uma direção-geral com 400 trabalhadores. É administração direta com 250 ou mais trabalhadores, portanto Grupo A, com quarenta medidas. O que leva mais tempo não é técnico: são as cinco políticas que o critério quer aprovadas e implementadas, e aprovar uma política envolve a direção. Começar por elas deixa a parte técnica para quando a política já diz o que a técnica tem de cumprir, e a política de acessos (O.PAP), por exemplo, é a referência expressa do critério de T.PAD.

A certificação como prova

O Regulamento presume o cumprimento das medidas quando a entidade tem uma certificação que as cubra, e para as entidades públicas relevantes nomeia o DNP TS 4577-1, o Selo Digital (Reg., art. 27.º, n.º 3). O CNCS pode também exigir uma certificação, por decisão fundamentada (RJC, art. 34.º, n.º 1). Sem certificação, a prova é a do critério de verificação, medida a medida.

Onde entramos

Não fazemos a qualificação nem a gestão do regime. Três critérios do Anexo IV pedem evidência técnica que produzimos. O critério de T.PEW, autenticação do correio eletrónico, protocolos seguros, certificados e cabeçalhos de segurança nas páginas, é o que o Buteo lê de fora em cada domínio. O inventário de O.IAC, na parte da rede, é o que o Ibex mantém por equipamento, incluindo nas redes sem ligação à internet. E o registo de atualizações de T.AS ganha uma verificação independente quando o Ibex lê a versão que cada serviço está realmente a correr.

O calendário completo do RJC, os prazos de notificação de incidentes e uma autoavaliação estão em NIS2 em Portugal: o RJC.

Verificado em 26 de setembro de 2026 contra o texto do Decreto-Lei n.º 125/2025 e do Regulamento n.º 756/2026 publicados no Diário da República. As medidas estão resumidas; em caso de dúvida, vale o texto do Anexo IV.

Fontes

- Decreto-Lei n.º 125/2025, de 4 de dezembro, que aprova o Regime Jurídico da Cibersegurança, Diário da República, 1.ª série, n.º 234: arts. 3.º, 6.º, 7.º, 9.º, 33.º, 34.º, 35.º, 40.º e 61.º do regime; art. 10.º do decreto-lei.
- Regulamento n.º 756/2026 do CNCS, Diário da República, 2.ª série, n.º 118, de 22 de junho de 2026: arts. 1.º, 27.º, 30.º e 35.º, e o Anexo IV, pp. 85 a 89.

Morada
Rua Major João Luís de Moura
Piso 1, Esc. AE · 1685-253 Famões

Contacto
hello@deltacoders.com

Web
deltacoders.com