

PRESIDÊNCIA DO CONSELHO DE MINISTROS**Resolução do Conselho de Ministros n.º 102/2026**

Sumário: Aprova o Plano Nacional de Nuvem Soberana e o respetivo Plano de Ação.

A transformação e reforma tecnológica do Estado constituem prioridades centrais do Programa do XXV Governo Constitucional, que visa posicionar Portugal entre os países digitalmente mais avançados da Europa, impulsionando uma Administração Pública mais eficiente, resiliente e preparada para os desafios da era digital.

A crescente relevância das infraestruturas digitais e dos dados para o funcionamento da economia, incluindo das instituições públicas, bem como o aumento dos riscos associados a fenómenos meteorológicos extremos, ao cibercrime e à guerra eletrónica, reforçam a necessidade de assegurar a soberania e a resiliência digital enquanto prioridade estratégica, a nível nacional e europeu.

Definindo soberania como o controlo do acesso aos dados e a garantia permanente de funcionamento de sistemas e infraestruturas críticas, esta é uma condição essencial para assegurar a continuidade dos serviços públicos, a segurança da informação e a autonomia de decisão do Estado. Assim sendo, cabe ao Estado criar condições para reforçar o papel de Portugal na oferta de serviços de computação em nuvem e de inteligência artificial soberanos.

Neste contexto, o Plano de Ação da Estratégia Digital Nacional para 2026-2027, aprovado pela Resolução do Conselho de Ministros n.º 214/2025, de 29 de dezembro, define medidas orientadas para o reforço das infraestruturas digitais do Estado, incluindo a criação de um plano de centralização e migração para soluções em nuvem (projeto 1.3), a definição de um modelo de classificação soberana dos dados da Administração Pública (projeto 8.2) e a elaboração de um plano para o desenvolvimento de uma nuvem soberana (projeto 13.1).

O Governo adota, por isso, uma visão integrada para o reforço das infraestruturas digitais do Estado, orientada para a construção de uma base tecnológica soberana, moderna, segura e resiliente que suporte a eficiência operacional da Administração Pública e a melhoria da qualidade dos serviços prestados aos cidadãos e às empresas.

Neste contexto, o Plano Nacional de Nuvem Soberana define a visão estratégica e linhas de ação para a adoção coordenada, transversal e segura de serviços de computação em nuvem na Administração Pública, em articulação com o Quadro de Soberania em Nuvem (Cloud Sovereignty Framework) da Comissão Europeia, e em alinhamento com o enquadramento legislativo nacional aplicável, nomeadamente o Decreto-Lei n.º 125/2025, de 4 de dezembro, que transpõe a Diretiva (UE) 2022/2555, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União, e a Estratégia Nacional de Segurança do Ciberespaço, aprovada pela Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho, e, bem assim, com o Quadro Nacional de Referência para a Cibersegurança.

O Plano Nacional de Nuvem Soberana pode também ser aplicável aos órgãos de soberania, com as necessárias adaptações e no respeito pela sua autonomia e atenta a natureza dos dados e sistemas que utilizam. Adicionalmente, e considerando a dimensão extraterritorial da Administração Pública, com adaptações concretas para a aplicação desta estratégia aos dados que têm origem em países terceiros.

Com este plano, o Governo posiciona Portugal na vanguarda da soberania digital europeia, em conformidade com as prioridades do Programa do XXV Governo Constitucional, e reforça a capacidade do Estado para proteger a sua informação estratégica, assegurar a continuidade dos serviços públicos e dispor de uma infraestrutura digital adequada aos desafios da transformação tecnológica, contribuindo simultaneamente para o desenvolvimento de uma economia digital mais dinâmica, inovadora e competitiva.

Assim:

Nos termos da alínea g) do artigo 199.º da Constituição, o Conselho de Ministros resolve:

1 – Aprovar o Plano Nacional de Nuvem Soberana (PNCS), constante do anexo à presente resolução e da qual faz parte integrante.

2 – Determinar que:

a) O financiamento da implementação da Nuvem Soberana, incluindo o processo de migração inicial, é garantido pelo orçamento do Estado através da Agência para a Reforma Tecnológica do Estado, I. P. (ARTE, I. P.), e da IP Telecom, S. A., podendo ser objeto de reforço via dotação centralizada das finanças;

b) O financiamento operacional com a Nuvem Soberana é preferencialmente suportado por receitas próprias da IP Telecom, S. A., resultantes das receitas pagas pelas entidades públicas e privadas que venham a utilizar a Nuvem Soberana;

c) As poupanças geradas nas entidades públicas pela utilização da Nuvem Soberana são partilhadas da seguinte forma: 30 % para a ARTE, I. P., 20 % para a IP Telecom, S. A., e 50 % para a respetiva entidade pública.

3 – Estabelecer que o acompanhamento e monitorização das medidas e ações estabelecidas na presente resolução são asseguradas pela Rede de Simplificação e Tecnologias do Estado, nos termos do Decreto-Lei n.º 85/2026, de 13 de abril.

4 – Mandatar a ARTE, I. P., e o Centro Nacional de Cibersegurança (CNCS) para, no prazo de 90 dias a contar da entrada em vigor da presente resolução, determinarem a metodologia de qualificação e os requisitos de soberania previstos na presente resolução, suportados por referencial técnico, e comunicarem-nos aos membros do Governo responsáveis pelas áreas da digitalização e da cibersegurança.

5 – Determinar que as entidades da Administração Pública procedem à qualificação dos seus processos com base no referencial técnico referido no número anterior, até 30 de junho de 2027, em articulação com a ARTE, I. P., e com o CNCS.

6 – Fixar que todas as orientações, guias, requisitos, referenciais técnicos e relatórios previstos na presente resolução são disponibilizados através do portal digital.gov.pt.

7 – Estabelecer que a presente resolução entra em vigor no dia seguinte ao da sua publicação.

Presidência do Conselho de Ministros, 14 de maio de 2026. — O Primeiro-Ministro, Luís Montenegro.

ANEXO

(a que se refere o n.º 1)

Plano Nacional de Nuvem Soberana

1 – Enquadramento estratégico

A Europa enfrenta um contexto global de fortes tensões geopolíticas e competição tecnológica, que aumentam os riscos sobre a sua autonomia, segurança e posição económica e estratégica. Neste quadro, a prioridade europeia centra-se no reforço da sua resiliência digital, garantindo o controlo e a segurança das tecnologias e infraestruturas críticas, sendo para isso essencial apostar na capacidade de resposta e na continuidade operacional face a potenciais disrupções.

Em matéria de nuvem soberana, é possível verificar que os países com maior maturidade na definição e implementação de estratégias nesta matéria partilham alguns princípios comuns, em particular:

- Dispõem de sistemas de qualificação de dados e de sistemas de informação, distinguindo explicitamente os críticos, e criam esquemas de credenciação (requisitos de segurança, soberania e conformidade) que influenciam a oferta;

- Adotam estratégias específicas de contratação (como contratos centralizados e acordos-quadro), simplificando procedimentos e reduzindo custos;

- Implementam estruturas de governação robustas, que coordenam políticas e asseguram consistência na execução; e

- Recorrem a modelos compostos por mais do que uma solução (infraestruturas de nuvem da Administração Pública, prestadores europeus certificados e provedores globais de serviços de nuvem em larga escala acreditados), dependendo da qualificação dos dados.

2 – A visão

Para assegurar que os sistemas do Estado têm um nível adequado de soberania, é necessário, num primeiro momento, qualificar os processos de negócio quanto à sua soberania e, posteriormente, identificar os requisitos necessários para garantir os níveis adequados de segurança, resiliência, controlo e eficiência operacional. Neste sentido, quanto maior for o impacto dos processos na soberania do Estado, maior será o grau de controlo a que esses processos, e respetivos dados e sistemas, devem estar sujeitos pelo setor público, garantindo-se assim o equilíbrio entre segurança, eficiência e soberania, condição essencial para a consolidação de uma soberania estruturalmente sustentável, financeiramente equilibrada e operacionalmente exequível.

O PNCS concretiza, no contexto nacional, uma estratégia de preferência pela utilização de soluções de computação em nuvem para as infraestruturas digitais do Estado, promovendo uma transição coordenada para plataformas mais seguras, resilientes e escaláveis. Esta abordagem permitirá aumentar a eficiência do setor público, acelerar a inovação e criar melhores condições para o desenvolvimento de serviços públicos digitais mais simples, integrados e centrados nas necessidades dos cidadãos e das empresas. Simultaneamente, o PNCS estabelece um modelo que assegura níveis adequados de soberania, segurança e resiliência digital, garantindo o controlo sobre dados, sistemas e infraestruturas críticas da Administração Pública.

Este modelo pode ser aplicável, com as necessárias adaptações e no respeito pelo princípio da separação e interdependência de poderes, aos órgãos de soberania, nos termos a concretizar nos respetivos Planos de Adoção Setoriais, com o envolvimento respetivo das entidades relevantes nesta matéria. Serão também consideradas as especificidades de cada área governativa na dimensão extra-territorial, nomeadamente as aplicáveis aos negócios estrangeiros.

3 – A abordagem

O Plano Nacional de Nuvem Soberana é executado através de uma metodologia estruturada, assente em três dimensões:

Dimensão 1 – Qualificação dos processos de negócio

A qualificação dos processos de negócio da Administração Pública, bem como dos dados e sistemas que os suportam, é um elemento central deste modelo. A informação é avaliada quanto à sua sensibilidade, criticidade e confidencialidade, determinando-se assim o nível de soberania necessário e os requisitos de segurança que devem ser observados.

Modelo e metodologia para a qualificação dos processos de negócio

O modelo de qualificação de processos permite aplicar níveis graduais de controlo em função da soberania dos processos de negócio, dos dados e dos sistemas de informação que os suportam. Neste contexto, os processos da Administração Pública devem ser qualificados em função do impacto que o comprometimento dos respetivos dados e sistemas tem para o funcionamento do Estado e para a prestação de serviços públicos.

Com base em referenciais internacionais e nas melhores práticas nacionais, o Centro Nacional de Cibersegurança (CNCS) e a Agência para a Reforma Tecnológica do Estado, I. P. (ARTE, I. P.), identificaram quatro níveis de qualificação de processos de negócio, aos quais corresponderão diferentes requisitos de soberania e controlo:

- Neutro — são processos que não estão sujeitos a requisitos, enquadrando-se no nível 0;

- Corrente — são processos que, não estando sujeitos a requisitos especiais de soberania, podem estar sujeitos a outros requisitos de soberania e segurança decorrentes da demais legislação aplicável, enquadrando-se no nível 1;

- Crítico — são processos que requerem o cumprimento de requisitos acrescidos, tanto de soberania como de segurança, podendo enquadrar-se no nível 2, correspondente à soberania de dados e operacional;

- Estratégico — são processos de natureza estratégica que exigem o cumprimento dos mais elevados requisitos de segurança e soberania, enquadrando-se no nível 3.a, associado à soberania de *software*, ou no nível 3.b, que corresponde à soberania de *software* de âmbito nacional.

Este modelo de qualificação de processos permitirá assegurar que os processos das entidades da Administração Pública, bem como os respetivos dados e sistemas que os suportam, são qualificados em função do impacto que o seu comprometimento tem na soberania nacional.

Para apoiar a aplicação deste modelo, o CNCS e a ARTE, I. P., procederão: i) à definição de um procedimento de pontuação de processos de negócio; e ii) à qualificação preliminar dos processos de negócio do 2.º nível do Catálogo de Processos de Negócio da Administração Pública, disponibilizado através da Plataforma de Classificação e Avaliação da Informação Pública (CLAV). O procedimento de pontuação de processos de negócio permitirá efetuar a pontuação dos processos do 2.º nível da CLAV com base em três dimensões:

1.1 — Pessoas e vida humana: Sem Impacto, Impacto Moderado ou Impacto Significativo;

1.2 — Estabilidade do Estado: Sem Impacto, Impacto Moderado ou Impacto Significativo;

1.3 — Exposição de Dados: Sem Impacto, Impacto Moderado ou Impacto Significativo.

A tabela de qualificação preliminar resultante deste exercício terá como objetivo acelerar e apoiar a qualificação a efetuar pelas entidades da Administração Pública. Sem prejuízo, as entidades da Administração Pública poderão efetuar a sua própria pontuação dos respetivos processos de negócio, com base no procedimento de pontuação de processos de negócio disponibilizado pelo CNCS e pela ARTE, I. P.

Em suma, a metodologia a adotar será:

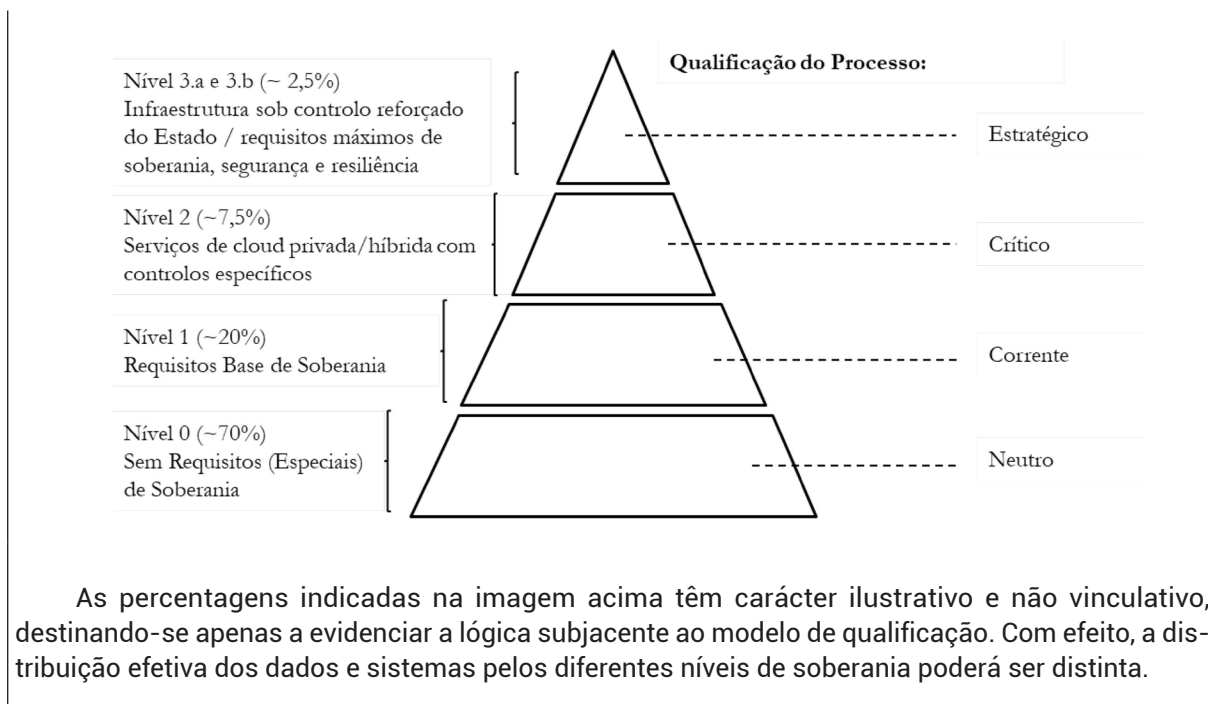
1) As entidades utilizarão a tabela de pré-qualificação a disponibilizar pelo CNCS e pela ARTE, I. P., para qualificarem os seus processos de negócio, identificando para cada processo qual o nível de soberania correspondente;

2) Na eventualidade de não concordarem com a pré-qualificação apresentada pelo CNCS e pela ARTE, I. P., as autoridades da Administração Pública poderão executar o procedimento de pontuação de processos de negócio, a disponibilizar pelo CNCS e pela ARTE, I. P.;

3) O resultado do processo de qualificação determinará o nível de soberania aplicável aos processos de negócios; e

4) Para cada nível de soberania, o CNCS e a ARTE, I. P., definirão um conjunto de requisitos de soberania e segurança a aplicar aos dados e sistemas que suportam os processos de negócio qualificados.

A experiência internacional demonstra que a grande maioria dos dados da Administração Pública tende a situar-se nos níveis com menores requisitos de soberania, enquanto uma pequena percentagem exige requisitos maiores de soberania e controlo.



Dimensão 2 – Definição de requisitos específicos de soberania e segurança

A cada nível de qualificação correspondem requisitos específicos de soberania, segurança e resiliência, os quais definem as condições técnicas e operacionais a cumprir pelas infraestruturas digitais e pelos serviços nuvem utilizados pelo Estado.

Dimensão 3 – Infraestruturas digitais soberanas

Os processos de negócio são priorizados em função das respetivas necessidades de soberania e, nesse sentido, é definido um plano de ação faseado para a adoção de soluções soberanas pelo Estado. Propõe-se, ainda, a compilação de uma oferta de infraestruturas digitais soberanas que responda aos diferentes níveis de exigência. Mais do que construir infraestrutura, o objetivo é criar condições para que o mercado funcione, assegurando que a oferta interna da Administração Pública e a oferta do mercado cumprem os requisitos de soberania e segurança.

4 – Plano de Ação

I – Infraestrutura digital soberana

Iniciativa	Descrição	Início	Entidades
I.1 – Modelo de qualificação dos processos de negócio	<p>Definição de um modelo uniforme de qualificação dos processos de negócio da Administração Pública, aplicável aos dados e sistemas de informação associados.</p> <p>Inclui categorias de processos, o respetivo enquadramento normativo, requisitos de soberania, segurança e resiliência por nível de qualificação e, ainda, especificações técnicas associadas a tais requisitos de soberania.</p> <p>Levantamento e inventariação dos processos e infraestruturas tecnológicas da Administração Pública, nomeadamente através da identificação e catalogação das dependências tecnológicas, vulnerabilidades e riscos.</p> <p>Aplicação do modelo de qualificação dos processos de negócio aos dados e sistemas inventariados.</p>	S1 2026	CNCS, ARTE, I. P., entidades da Administração Pública envolvidas no processo de inventariação

Iniciativa	Descrição	Início	Entidades
I.2 – Desenvolvimento da Oferta de Nuvem Soberana, incluindo inteligência artificial (IA)	Desenvolvimento, pelo Estado, de infraestrutura nacional soberana de nuvem, incluindo capacidades de IA soberana. Criação de um catálogo unificado de serviços de nuvem que permita a consulta das ofertas de nuvem disponíveis para a Administração Pública.	S1 2026	ARTE, I. P, CNCS, Entidade de Serviços Partilhados da Administração Pública, I. P. (ESPAP, I. P.) e IP Telecom, Serviços de Telecomunicações, S. A., entidades da Administração Pública utilizadoras da infraestrutura soberana do Estado
I.3 – Plano de Adoção da Nuvem Soberana	Revisão do Framework de Adoção na Nuvem, enquanto componente do MOSAICO, incorporando os princípios do PNCS. Definição de orientações práticas para apoiar as entidades da Administração Pública na tomada de decisão sobre migração, modernização ou manutenção de sistemas. Elaboração de planos de adoção setoriais para cada área governativa, estabelecendo projetos, atividades, responsabilidades, calendarização e metas para a adoção da arquitetura tecnológica de soberania definida no PNCS. Execução e acompanhamento dos planos de adoção setoriais.	S2 2026	ARTE, I. P., CNCS, áreas governativas e respetivas entidades sob sua tutela
I.4 – Definição de um acor-do-quadro para serviços de nuvem	Análise comparativa aos modelos de contratação pública para serviços de nuvem adotados a nível internacional. Definição de princípios, diretrizes e modelos de aquisição comuns para serviços de nuvem aplicáveis a todas as entidades da Administração Pública. Definição de cláusulas-tipo, requisitos de segurança, níveis de serviço exigidos (SLAs) e guias operacionais.	S1 2027	ARTE, I. P., ESPAP, I. P., CNCS

II – Capacitação de recursos humanos

Iniciativa	Descrição	Início	Entidades
II.1 – Matriz de competências para a Nuvem Soberana	Identificação dos perfis técnicos e funcionais necessários para a implementação, operação e manutenção da Nuvem Soberana na Administração Pública. Construção de uma matriz para cada perfil, que identifique as competências técnicas e funcionais necessárias à sua função, nível de proficiência exigido, bem como formações e certificações recomendadas.	S2 2026	ARTE, I. P., Instituto Nacional de Administração, I. P. (INA, I. P.), Direção-Geral da Administração e do Emprego Público (DGAEP)
II.2 – Plano de Capacitação em Soberania Digital	Definição de um programa de formação em soberania digital para a Administração Pública, dirigido aos perfis técnicos e funcionais mapeados na iniciativa I.1. Formação de, pelo menos, 10 % dos especialistas de informática da Administração Pública em soberania digital até 2028. Formação de, pelo menos, 1000 dirigentes e gestores de projeto da Administração Pública em soberania digital até 2030. Definição de um plano de iniciativas de partilha de conhecimento, incluindo sessões regulares de capacitação e troca de experiências entre entidades públicas que utilizem a Nuvem Soberana.	S2 2026	ARTE, I. P., INA, I. P., Agência para a Investigação e Inovação (AI ²), E. P. E., instituições de ensino superior, outras entidades relevantes

III – Alterações legislativas

Iniciativa	Descrição	Início	Entidades
III.1 – Simplificação e revisão do processo de aquisição de serviços nuvem	Eliminação de barreiras burocráticas associadas à aquisição de serviços nuvem, promovendo a agilidade na contratação e a abertura do mercado a fornecedores mais diversificados e a soluções de nuvem, com impacto positivo na qualidade e eficiência dos serviços prestados. Análise da possibilidade de reenquadramento orçamental das compras de serviços de nuvem.	S1 2026	Governo de Portugal
III.2 – Elegibilidade financeira dos serviços de computação em nuvem	Estabelecimento de condições e critérios claros para garantir que serviços de computação em nuvem possam ser elegíveis para linhas de financiamento nacionais e europeias. Análise de implicações em matéria de tratamento contabilístico dos serviços de computação em nuvem, permitindo a sua classificação como investimentos produtivos, quando associados à transformação tecnológica e à criação de valor público.	S2 2026	Governo de Portugal

119948632