OBSERVATÓRIO DOS ECOSSISTEMAS E INFRAESTRUTURAS DIGITAIS

05/2025

25 Medidas Estratégicas para a criação da Cloud Soberana da Administração Pública Portuguesa

CONTRIBUTO DO OBSERVATÓRIO DOS ECOSSISTEMAS E INFRAESTRUTURAS DIGITAIS (OEID) – AGENDA DIGITAL NACIONAL

COORDENAÇÃO: RUI RIBEIRO (CONSELHO CONSULTIVO)

MAIO DE 2025 - PORTUGAL

Índice

INTRODUÇÃO

A transformação digital do Estado é hoje uma prioridade nacional e europeia, com impactos diretos na soberania, eficiência administrativa e confiança dos cidadãos nas instituições. Face aos desafios da cibersegurança, fragmentação tecnológica, dependência externa e escassez de recursos especializados, Portugal deve dar um passo firme no sentido da criação de uma Cloud Soberana da Administração Pública, assegurando o controlo sobre os seus dados e sistemas críticos.

Neste enquadramento, o Observatório dos Ecossistemas e Infraestruturas Digitais (OEID) apresenta uma proposta estratégica composta por 25 medidas fundamentais, com o objetivo de garantir uma infraestrutura tecnológica centralizada, segura, escalável e capaz de sustentar a modernização da Administração Pública. Esta cloud será gerida por uma nova entidade pública – a **Agência Nacional Digital (AND)** – resultante da fusão da Agência para a Modernização Administrativa (AMA), da Entidade de Serviços Partilhados da Administração Pública (ESPAP) e do Instituto de Informática da Segurança Social (IISS), agregando competências em gestão de infraestruturas, interoperabilidade e contratação digital.

As propostas estão organizadas em cinco eixos estratégicos, que estruturam a visão de futuro para uma Administração Pública mais digital, soberana e resiliente:

A. Governação e Organização da Cloud Soberana
Define a criação de estruturas institucionais e legais robustas, com liderança centralizada, modelo de governação claro e envolvimento de diferentes stakeholders na definição de prioridades e políticas.

B. Infraestrutura e Soberania Tecnológica
Estabelece os princípios de localização dos dados em território nacional, construção ou certificação de datacenters públicos, adoção de uma arquitetura cloud híbrida interoperável e criação de um marketplace de serviços cloud.

C. Transformação Digital e Modernização dos Serviços Públicos
Aponta caminhos para a digitalização total dos serviços, desmaterialização de processos, integração de camadas IaaS, PaaS e SaaS, automação com IA e reforço do portal único do Estado como interface central.

D. Cibersegurança, Continuidade de Negócio e Sustentabilidade Digital
Introduz mecanismos de segurança baseados no modelo Zero Trust, criação de um centro nacional de cibersegurança para a cloud, planos de continuidade operacional e sustentabilidade energética dos datacenters.

E. Capacitação, Inovação e Cooperação Internacional
Reforça a importância da formação de quadros públicos, integração da cloud nos currículos educativos, criação de um laboratório de inovação pública e alinhamento com a estratégia europeia de dados e cloud.

A Cloud Soberana da Administração Pública não é apenas uma infraestrutura tecnológica – é uma nova fundação para o Estado digital português. Um projeto transformador, colaborativo e alinhado com os valores europeus de autonomia estratégica, inovação sustentável e proteção dos direitos dos cidadãos. Este documento constitui um contributo técnico e estratégico para a sua concretização.

AS 25 MEDIDAS ESTRATÉGICAS 25 MEDIDAS PARA A CRIAÇÃO DA CLOUD SOBERANA DA ADMINISTRAÇÃO PÚBLICA PORTUGUESA

Eixo A - Governação e Organização da Cloud Soberana da Administração Pública

Medida 1: Criação da Agência Nacional Digital (AND) e da Estrutura de Soberania Digital e Segurança da Informação (ESDSI)

A criação da **Agência Nacional Digital (AND)** representa uma medida estratégica essencial para consolidar a transformação digital do Estado português e reforçar o seu papel como motor do desenvolvimento económico e da capacitação digital da sociedade. A AND deverá resultar da fusão da **Agência para a Modernização Administrativa (AMA)**, da **Entidade de Serviços Partilhados da Administração Pública (ESPAP)** e do **Instituto de Informática da Segurança Social (IISS)**, integrando competências em **infraestruturas digitais, interoperabilidade, contratação pública digital, transformação organizacional e inovação tecnológica**.

A AND será o **organismo central de governação da Cloud Soberana da Administração Pública**, com autoridade para definir normas técnicas, promover a modernização dos serviços públicos, assegurar a conformidade com regulamentos europeus e implementar soluções tecnológicas escaláveis e centradas no cidadão. Para além das funções operacionais, a AND terá também um mandato claro de **estimular o desenvolvimento económico**, através da articulação com o setor privado, universidades, startups e centros de inovação, promovendo uma economia digital mais inclusiva e competitiva.

A liderança da AND assumirá as funções de um modelo similar ao perfil de **Chief Information Officer (CIO) do Estado**, garantindo coerência estratégica, coordenação interministerial e alinhamento tecnológico em toda a Administração Pública. Neste sentido, a AND deverá **absorver as funções de governação estratégica atualmente dispersas por várias entidades IT da Administração Pública Setorial**, como a SPMS (Saúde), o IGFEJ (Justiça) e a AT (Finanças), nomeadamente em matérias de **políticas digitais, procurement, gestão de recursos humanos e planeamento tecnológico**.

As componentes **operacionais de primeira linha** (como apoio local, suporte de utilizador ou manutenção de proximidade) deverão manter-se **descentralizadas e sob responsabilidade das entidades setoriais**, mas articuladas com a estratégia definida pela AND. A **Cloud Soberana**, enquanto infraestrutura comum e transversal, será **um promotor natural deste modelo**, facilitando a centralização da governação tecnológica e garantindo ao mesmo tempo flexibilidade na execução setorial.

Paralelamente, deverá ser criada uma estrutura autónoma e de alto nível – a **Estrutura de Soberania Digital e Segurança da Informação (ESDSI)** – diretamente dependente do Governo, com foco exclusivo na **segurança da informação**, incluindo **cibersegurança, proteção de informação classificada e resiliência digital do Estado**. Esta estrutura será responsável pela definição de políticas e normas de segurança, pela vigilância ativa das infraestruturas críticas e pela resposta a incidentes de segurança em todo o ecossistema público.

A ESDSI será a sede operacional do **CERT.PT (Computer Emergency Response Team)** da Administração Pública, e integrará ainda os **centros nacionais de operações de segurança (SOC) e de rede (NOC) do Estado**.

Importa reforçar que o **Centro Nacional de Cibersegurança (CNCS)** se manterá no seu papel institucional como entidade nacional de referência para a cibersegurança, com funções de definição estratégica, promoção de boas práticas, regulamentação técnica e articulação com parceiros internacionais e entidades privadas. A atuação da ESDSI será complementar, com foco operacional e específico na segurança da Administração Pública e das infraestruturas críticas do Estado.

Esta medida sistematiza duas lideranças estratégicas:

- O papel de **Chief Information Officer (CIO)** do Estado, preconizado pela AND, responsável por garantir a coerência estratégica, a coordenação interministerial e o alinhamento tecnológico em toda a Administração Pública, assegurando a arquitetura digital e a orientação para a inovação tecnológica da AP.
- O papel desempenhado pela **ESDSI como Chief Information Security Officer (CISO)** do Estado, com a missão de supervisionar a cibersegurança, a gestão de riscos, a proteção da informação e a resposta a incidentes em todo o ecossistema digital público.

Estas funções, inexistentes de forma integrada até hoje, são críticas para afirmar a liderança e a responsabilização estratégica da Administração Pública no contexto da **soberania digital, da resiliência cibernética e da confiança dos cidadãos**.

Medida 2: Constituição de uma equipa de Gestão Central multidisciplinar

A operacionalização da Cloud Soberana requer uma **equipa de gestão central multidisciplinar**, composta por perfis altamente qualificados em áreas como engenharia de sistemas, arquitetura cloud, cibersegurança, interoperabilidade, gestão de projetos e políticas públicas digitais. Esta equipa deve operar dentro da AND, com competências executivas para planeamento, implementação, monitorização e evolução contínua da cloud.

A profissionalização e estabilidade desta equipa será essencial para garantir a continuidade estratégica do projeto, a gestão de fornecedores e a coordenação com organismos setoriais. Adicionalmente, deverá ser criada uma estrutura de governance baseada em princípios de transparência, accountability e colaboração com outras entidades públicas, academia e indústria.

Medida 3: Definição de um Quadro Legal e Normativo para a Cloud Soberana

A Cloud Soberana necessita de um **quadro legal específico**, adaptado aos desafios da proteção de dados, segurança nacional, interoperabilidade europeia e sustentabilidade tecnológica. Este enquadramento deve ser criado em articulação com a Comissão Europeia, assegurando alinhamento com as normas do European GAIA-X, do European Data Governance Act e do Cybersecurity Act.

O novo quadro jurídico deve garantir o **controlo nacional sobre os dados da Administração Pública**, impor que os dados estejam alojados em datacenters em território nacional (com cópias de segurança secundárias em clouds soberanas europeias), e definir regras para contratação pública de serviços digitais em modelo cloud, privilegiando fornecedores que cumpram requisitos de soberania, segurança e sustentabilidade.

Medida 4: Reforço e Alargamento do Conselho para o Digital na Administração Pública (CDAP)

O **Conselho para o Digital na Administração Pública (CDAP)**, já existente, deve ser **reforçado e reposicionado como órgão consultivo estratégico** da governação da Cloud Soberana da Administração Pública e da transformação digital do Estado. A sua atuação deve ganhar maior abrangência, regularidade e capacidade de influência sobre a definição de prioridades tecnológicas, avaliação de projetos críticos e validação de políticas públicas digitais.

Este conselho deverá integrar, além das entidades públicas com competências em tecnologias da informação, **representantes da academia, do setor privado, de centros**

de investigação e da sociedade civil, garantindo uma visão plural e independente sobre a evolução do ecossistema digital do Estado. A sua missão passará a incluir a **emissão de pareceres estratégicos**, a avaliação do cumprimento de metas de transformação digital, e a promoção de princípios de **transparência, interoperabilidade e ética digital**.

Ao ser formalmente envolvido na estrutura de governação da Cloud Soberana – com articulação direta com a Agência Nacional Digital (AND) e reporte ao Governo –, o CDAP ganha relevância institucional como **espaço de auscultação, orientação estratégica e legitimação pública** das decisões sobre o futuro digital do Estado português.

Medida 5: Definição de um Plano Diretor da Cloud Soberana da Administração Pública

A definição de um **Plano Diretor da Cloud Soberana** é fundamental para estruturar as fases de desenvolvimento, adoção e expansão dos serviços cloud na AP. Este plano deverá definir objetivos de curto, médio e longo prazo, cronogramas de migração, modelos de serviço (IaaS, PaaS, SaaS), métricas de desempenho, requisitos técnicos e operacionais, bem como o modelo de investimento e financiamento da infraestrutura.

O plano diretor permitirá alinhar todas as entidades públicas com uma visão comum, garantir transparência nos investimentos, e estabelecer prioridades conforme a criticidade e maturidade digital dos organismos da AP. Deve ser atualizado periodicamente e articulado com a Estratégia Portugal Digital e com os instrumentos financeiros do PRR, PT2030 e fundos europeus.

Eixo B - Infraestrutura e Soberania Tecnológica

Medida 6: Localização exclusiva dos Dados da Administração Pública em Datacenters nacionais, com valorização de instalações de elevada segurança

A concretização da soberania digital da Administração Pública exige que **todos os dados e sistemas críticos do Estado estejam obrigatoriamente alojados em datacenters situados em território português**, operados por entidades públicas ou por parceiros estratégicos que cumpram os requisitos de soberania definidos pela Agência Nacional Digital (AND). Esta medida garante **controlo jurídico, técnico e geoestratégico total sobre os dados do Estado**, protegendo-os de interferência externa e assegurando a sua gestão de acordo com os interesses nacionais.

Para garantir **resiliência e continuidade de serviço**, os dados deverão ser replicados em **vários datacenters nacionais geograficamente distribuídos**. Em situações de missão crítica, poderá ainda ser considerada a existência de cópias de segurança secundárias em clouds soberanas de outros Estados-membros da União Europeia, desde que exista controlo contratual sobre o acesso, reversibilidade garantida e conformidade com a legislação europeia e nacional.

De forma complementar, propõe-se a **valorização estratégica de instalações militares como locais prioritários para a instalação de datacenters de elevada criticidade**, beneficiando das condições já existentes de segurança física, controlo de acessos, certificações internacionais e capacidade de defesa ativa. A sediação de datacenters em unidades militares representaria não só um reforço da proteção dos ativos digitais do Estado, mas também uma oportunidade de investimento direto na modernização da Defesa e Segurança, nomeadamente em áreas como abastecimento energético, redundância de conectividade, capacitação técnica e requalificação das infraestruturas.

Esta medida criaria igualmente novas vias **de cooperação entre o setor da Defesa, a sociedade civil e a Academia**, permitindo que estas infraestruturas funcionem também como polos de formação, estágios e integração profissional para jovens engenheiros e técnicos especializados, promovendo experiências híbridas entre percursos profissionais civis e contextos de missão pública. A utilização de recursos humanos militares e civis qualificados contribuiria para consolidar uma cultura de excelência, disciplina e responsabilidade no tratamento da informação mais sensível do Estado.

Medida 7: Construção ou Certificação de uma Rede Nacional de Datacenters Públicos

Para implementar a Cloud Soberana, é essencial dispor de uma **rede nacional de datacenters públicos**, interoperáveis e com elevada resiliência energética, física e digital. Esta rede pode resultar da **construção de novos datacenters** estratégicos, ou da

certificação e adaptação de infraestruturas já existentes em organismos do Estado, forças armadas, universidades ou operadores públicos de serviços essenciais.

A criação de uma rede federada permite equilibrar custos, reduzir redundâncias e promover a sustentabilidade. Todos os datacenters deverão seguir **normas de eficiência energética**, segurança física, conformidade com o RGPD, e suportar uma arquitetura de cloud híbrida que integre capacidades IaaS, PaaS e SaaS sob gestão da AND.

Medida 8: Adoção de Arquitetura Cloud Híbrida com Interoperabilidade Europeias

A Cloud Soberana da AP deve assentar numa **arquitetura híbrida**, que permita conjugar a segurança e controlo dos datacenters nacionais com a **capacidade de integração com outras clouds soberanas europeias**. Esta abordagem garante escalabilidade, inovação e continuidade de negócio, em alinhamento com iniciativas similares como o **GAIA-X** e o **European Interoperability Framework**.

A arquitetura híbrida permitirá também explorar **cenários de disaster recovery e continuidade de serviços**, com backups ou cargas de trabalho secundárias migráveis para clouds europeias em caso de catástrofes. Todos os serviços devem ser desenhados com base em APIs abertas e interoperáveis, promovendo portabilidade, flexibilidade e inovação futura.

Medida 9: Criação de Marketplace Nacional de Serviços Cloud Públicos

Para facilitar a adoção da Cloud Soberana, propõe-se a criação de um **Marketplace Nacional de Serviços Cloud Públicos**, onde os organismos da AP poderão aceder a um catálogo validado de soluções IaaS, PaaS e SaaS, desenvolvidas pela AND ou por parceiros tecnológicos certificados. O marketplace permitirá acelerar a digitalização, assegurando qualidade, segurança e conformidade.

Este modelo facilita a aquisição de serviços sob um regime contratual centralizado, reduzindo a fragmentação e melhorando o controlo financeiro. O marketplace deverá incluir soluções horizontais (como email, armazenamento, análise de dados, gestão documental) e verticais (ex: saúde, educação, justiça), alinhadas com as necessidades dos organismos públicos.

Medida 10: Definição de normas técnicas para Interoperabilidade e Reversibilidade

Um dos pilares da soberania digital é garantir a **interoperabilidade entre sistemas** e a **reversibilidade contratual e tecnológica**. Assim, a AND deverá definir um conjunto de

normas técnicas obrigatórias que assegurem a portabilidade dos dados, a compatibilidade entre plataformas, a abertura de APIs e a capacidade de migrar serviços sem lock-in tecnológico.

Estas normas serão aplicáveis a todos os fornecedores de soluções digitais para a Administração Pública, com certificações exigidas para participação no marketplace nacional. A adoção de standards abertos e auditáveis permitirá garantir a confiança nos sistemas, facilitar a integração entre organismos e assegurar a autonomia estratégica da AP portuguesa.

Eixo C - Transformação Digital e Modernização dos Serviços Públicos

Medida 11: Digitalização total dos Serviços Públicos com prioridade na desmaterialização de processos

A Cloud Soberana deve ser o pilar tecnológico para a **transformação digital integral da Administração Pública**, com enfoque na **desmaterialização de processos**, eliminação do papel, automatização de tarefas repetitivas e integração entre serviços. A meta é permitir que qualquer cidadão ou empresa possa interagir com o Estado de forma 100% digital, acessível, segura e transparente.

Os organismos públicos deverão ser apoiados pela AND para mapear os seus processos internos, identificar ineficiências, redesenhar fluxos e adotar soluções digitais baseadas em plataformas da Cloud Soberana. A prioridade será dada a serviços de alto impacto como licenciamento, apoios sociais, justiça, saúde e educação.

Medida 12: Adoção obrigatória da Cloud Soberana por toda a Administração Pública e definição de plano de migração

A Cloud Soberana deverá ser **a infraestrutura tecnológica de referência e de utilização obrigatória** por parte de **toda a Administração Pública**, incluindo organismos da administração **central, local e setorial**. Esta medida visa garantir a uniformização de práticas, a segurança da informação, a eficiência dos investimentos e a interoperabilidade entre sistemas públicos.

A **Agência Nacional Digital (AND)** será responsável por coordenar, em articulação com os diferentes ministérios, câmaras municipais, institutos e serviços públicos, a elaboração de um **Plano Nacional de Migração para a Cloud Soberana**, que identifique os **serviços elegíveis** para transição, as **prioridades por setor**, os **requisitos técnicos**, e os **prazos máximos de adaptação**. A migração será faseada, com metas anuais e mecanismos de apoio técnico para os organismos com menor capacidade interna.

A obrigatoriedade da adoção deverá ser acompanhada por **critérios claros de exceção** (casos justificados de autonomia tecnológica, requisitos legais ou operacionais específicos) e por **instrumentos de financiamento e capacitação** adequados. Esta medida garantirá que a Cloud Soberana se afirme como uma **plataforma pública comum e transversal**, capaz de suportar de forma segura, eficiente e evolutiva os serviços digitais de todo o Estado português.

Medida 13: Automação de serviços públicos com IA, RPA e Análise Preditiva

A Cloud Soberana deverá incluir **capacidades nativas de automação**, incorporando tecnologias como Inteligência Artificial (IA), Robotic Process Automation (RPA) inteligentes (segunda geração) e análise preditiva. Estas tecnologias permitirão otimizar o funcionamento da máquina pública, reduzir tempos de resposta, libertar recursos humanos para tarefas de maior valor e personalizar os serviços ao cidadão.

A AND deve disponibilizar um conjunto de ferramentas e APIs baseadas nestas tecnologias, em conformidade com os princípios éticos da IA da UE. A aplicação prática incluirá desde bots de atendimento automático e triagem inteligente de pedidos, até modelos de previsão de procura por serviços ou gestão preditiva de infraestruturas públicas.

Medida 14: Reforço do portal único do Estado (gov.pt) como Interface Digital Central

O Portal Único do Estado deverá ser consolidado como a plataforma central de interação digital entre o Estado, os cidadãos e as empresas, agregando todos os serviços públicos digitais sob uma única experiência de utilizador, com navegação intuitiva, linguagem acessível e arquitetura de conteúdos centrada na vida do cidadão.

Neste contexto, será implementada a obrigatoriedade de que todos os organismos da Administração Pública – centrais, locais e setoriais – operem exclusivamente sob o domínio ".gov.pt", garantindo a identidade digital unificada do Estado. Esta medida assegura maior confiança, segurança, coerência comunicacional e facilita o reconhecimento e acesso por parte dos cidadãos.

A Cloud Soberana suportará integralmente a infraestrutura do portal e dos subdomínios associados, assegurando **resiliência, escalabilidade e integração com serviços transversais** como autenticação federada (Chave Móvel Digital), notificações proativas, histórico de interações, e recomendação de serviços relevantes. A medida representa um passo decisivo para posicionar o Estado como **uma única entidade digital, moderna, acessível e confiável**.

Medida 15: Integração da Cloud com a Estratégia de Dados da Administração Pública

A transformação digital não se esgota na digitalização de processos: deve ser alicerçada numa **estratégia de dados transversal**, que a Cloud Soberana permitirá operacionalizar. A infraestrutura cloud da AND deve suportar a criação de **lakes de dados públicos**, com mecanismos robustos de catalogação, anonimização, partilha segura e interoperabilidade entre organismos.

A integração com o sistema nacional de interoperabilidade será essencial para promover a **eficiência administrativa, prevenção de fraudes, planeamento de políticas públicas baseadas em evidência** e para fomentar a inovação através do acesso controlado a dados por investigadores, empresas e startups. A Cloud será a fundação digital dessa nova inteligência pública.

Eixo D - Cibersegurança, Continuidade de Negócio e Sustentabilidade

Medida 16: Adoção de um modelo Zero-Trust para toda a Cloud Soberana

A segurança da Cloud Soberana deverá assentar num **modelo de segurança "Zero Trust"**, que assume que nenhuma entidade, interna ou externa, é automaticamente confiável. Este paradigma requer autenticação contínua, segmentação de redes, monitorização constante e gestão rigorosa de identidades, acessos e permissões.

A AND deverá definir uma arquitetura de referência baseada em Zero Trust para toda a infraestrutura cloud, incluindo a implementação obrigatória de multifator de autenticação (MFA), encriptação ponta-a-ponta, auditorias contínuas e gestão de riscos por comportamento anómalo. Este modelo garantirá um patamar elevado de resiliência contra ciberataques e acessos indevidos.

Medida 17: Implementação de um Centro Nacional de Operações de Cibersegurança para a Cloud Soberana

No âmbito da Estrutura Nacional de Soberania Digital e Segurança da Informação (ENDSI), será criada uma estrutura operacional robusta de resposta e monitorização contínua, através **da implementação de um Centro Nacional de Operações de Cibersegurança, ao serviço da Administração Pública e das infraestruturas críticas do Estado**. Esta medida reforça a capacidade do Estado português para antecipar, detetar, responder e recuperar perante ameaças digitais, num contexto de risco geopolítico e tecnológico crescente.

O centro será constituído por uma estrutura técnica permanente integrada na ESDSI, responsável pela coordenação dos recursos de segurança operacional, vigilância ativa, deteção de anomalias, resposta a incidentes, análise forense e threat intelligence. Este centro incorporará e consolidará o funcionamento dos atuais SOC (Security Operations Center) e CERT.PT, operando em articulação com o CNCS, as Forças de Segurança e os centros congéneres da União Europeia.

A sua missão será também a de garantir a **execução técnica e operacional da ENDSI**, assegurando que todos os organismos da Administração Pública cumprem normas de cibersegurança, participam em exercícios de simulação de resposta a incidentes, e beneficiam de apoio preventivo e corretivo. A Cloud Soberana funcionará como infraestrutura crítica para esta capacidade de defesa digital, integrando os mecanismos automatizados de monitorização e controlo de risco.

Medida 18: Plano Nacional de Continuidade e Recuperação de Serviços Críticos da Administração Pública

Será estabelecido um Plano Nacional de Continuidade de Negócio e Recuperação de Desastres (PNCRD), com base na Cloud Soberana. O plano definirá protocolos específicos para serviços críticos da Administração Pública, assegurando a manutenção de operações essenciais mesmo em caso de falha total de sistemas, ataques cibernéticos ou catástrofes naturais.

Este plano incluirá mecanismos automáticos de failover, replicação de dados em datacenters redundantes e simulações periódicas de incidentes, para testar a capacidade de resposta dos organismos. A Cloud Soberana funcionará assim como o garante digital da continuidade institucional do Estado.

Medida 19: Sustentabilidade Energética dos Datacenters Públicos da Cloud Soberana

A estratégia da Cloud Soberana deve incorporar desde a origem princípios de sustentabilidade ambiental, reduzindo a pegada energética e promovendo a transição verde. Os datacenters públicos utilizados deverão cumprir requisitos mínimos de eficiência energética (ex. PUE abaixo de 1.3) e preferencialmente operar com energia de fontes renováveis.

Adicionalmente, serão promovidas boas práticas de gestão energética, como a utilização de sistemas de arrefecimento inovadores, reaproveitamento de calor residual e otimização da ocupação de recursos computacionais. A sustentabilidade será um critério de certificação e seleção de infraestruturas cloud no ecossistema da AND.

Medida 20: Reforço do Observatório de Cibersegurança em articulação com a ESDSI e a Cloud Soberana

O Observatório de Cibersegurança, atualmente em funcionamento no âmbito do Centro Nacional de Cibersegurança (CNCS), deve ser reforçado enquanto instrumento técnico e estratégico de apoio à monitorização da resiliência digital do Estado, especialmente no contexto da implementação da Cloud Soberana e da Estratégia Nacional de Soberania Digital e Segurança da Informação (ENDSI).

Este reforço passa por uma **articulação estruturada entre o CNCS, a ESDSI e a Agência Nacional Digital (AND)**, de modo a assegurar que o Observatório tem acesso continuado a dados estatísticos, indicadores de risco, métricas de conformidade e informação sobre incidentes relevantes nos sistemas da Administração Pública. A infraestrutura da Cloud Soberana permitirá recolher e integrar dados operacionais relevantes de forma sistematizada e segura.

A missão do Observatório deverá incluir a **produção periódica de relatórios públicos e técnicos**, estudos comparativos, recomendações de boas práticas e alertas setoriais, funcionando como uma **fonte confiável de inteligência sobre o estado da cibersegurança nacional**. A colaboração com universidades, centros de investigação e entidades europeias deverá ser aprofundada, reforçando o seu papel enquanto plataforma de conhecimento e base de evidência para a melhoria contínua da segurança digital do Estado.

Eixo E - Capacitação, Inovação e Cooperação Internacional

Medida 21: Programa Nacional de Capacitação para a Cloud na Administração Pública

A adoção da Cloud Soberana requer uma **profunda capacitação dos recursos humanos da Administração Pública**. A AND deverá lançar um **Programa Nacional de Capacitação**, em parceria com universidades, institutos politécnicos e centros de formação especializados, destinado a formar técnicos, dirigentes e decisores públicos nos modelos cloud, cibersegurança, gestão de dados, interoperabilidade e inovação digital.

O programa deverá incluir formações modulares, presenciais e online, com certificação, e abranger diferentes níveis de complexidade, desde utilizadores até arquitetos de sistemas. Esta medida garantirá a **sustentabilidade da estratégia cloud a longo prazo**, evitando dependência externa e promovendo uma nova cultura digital no setor público.

Medida 22: Criação de um laboratório de inovação pública baseado na Cloud Soberana

Para estimular a experimentação, prototipagem e aceleração de novas soluções digitais, propõe-se a criação de um **Laboratório de Inovação Pública** (GovTech Lab), suportado pela Cloud Soberana. Este laboratório atuará como plataforma para testes controlados de novas tecnologias, desenvolvimento de serviços digitais orientados ao cidadão e validação de ideias-piloto em ambientes reais.

A infraestrutura cloud permitirá testar soluções de IA, IoT, realidade aumentada, blockchain e outras tecnologias emergentes, em colaboração com startups, empresas estabelecidas, instituições de ensino superior e centros de I&D. A AND poderá lançar desafios públicos (Gov Challenges), promovendo a cocriação entre o Estado e o ecossistema de inovação.

Medida 23: Inclusão da Cloud Soberana no currículo do Ensino Superior e Profissional

A consolidação da soberania digital em Portugal implica integrar o tema da **Cloud Soberana e da transformação digital do Estado** nos planos curriculares do ensino superior e da formação profissional. A AND, em articulação com o Ministério da Educação, deverá propor conteúdos curriculares e módulos formativos específicos.

Estas ações promoverão a criação de **novas gerações de profissionais preparados para trabalhar com soluções cloud seguras, éticas e sustentáveis**, e ajudarão a posicionar Portugal como referência em competências digitais no contexto europeu. A disseminação do conhecimento contribuirá ainda para a literacia digital dos cidadãos.

Medida 24: Alinhamento com a Estratégia Europeia de Cloud e cooperação com outras Clouds soberanas

A Cloud Soberana portuguesa deverá ser concebida desde a origem em **alinhamento com a Estratégia Europeia de Dados e Cloud**, participando ativamente em iniciativas como o **GAIA-X**, **European Cloud Federation** e projetos comuns de interoperabilidade e partilha de recursos com outros Estados-Membros.

A AND deverá estabelecer **acordos de cooperação técnica e política com clouds soberanas de países parceiros**, garantindo que os dados de backup secundário sejam armazenados em infraestruturas confiáveis, dentro da UE. Esta medida assegura a resiliência da Cloud Soberana e a integração de Portugal na nova geopolítica digital europeia.

Medida 25: Campanha nacional de comunicação sobre soberania digital e confiança no Estado Digital

Por fim, propõe-se o lançamento de uma **campanha nacional de sensibilização e comunicação** sobre a importância da Cloud Soberana, soberania digital e confiança nos serviços públicos digitais. Esta campanha deverá ser coordenada pela AND, com o objetivo de informar os cidadãos sobre a segurança, acessibilidade e benefícios dos serviços digitais estatais.

A comunicação deve utilizar canais diversificados e linguagem clara, promovendo o envolvimento cívico e a literacia digital. A confiança dos cidadãos é um ativo estratégico para o sucesso da transformação digital, e será fundamental mostrar que a Cloud Soberana é **um investimento na autonomia, segurança e modernidade de Portugal**.

Recomendações Finais

A construção de uma Cloud Soberana para a Administração Pública Portuguesa representa uma oportunidade única para reposicionar o Estado como ator central na transformação digital, reforçar a sua autonomia estratégica e garantir a confiança dos cidadãos nos serviços públicos digitais. Ao longo deste documento foram apresentadas 25 medidas concretas, organizadas em cinco eixos estruturantes, que oferecem uma base sólida para a concretização desta visão nacional.

Com base na análise e propostas desenvolvidas, destacam-se as seguintes recomendações finais:

1. Iniciar de imediato o processo legislativo e institucional para a criação da Agência Nacional Digital (AND), assegurando a sua constituição legal, o seu modelo de governação e a integração funcional da AMA, ESPAP e IISS. A AND deverá concentrar as funções estratégicas de governação digital, assumindo o papel de CIO do Estado e atuando como pilar central da estratégia cloud e da modernização tecnológica da Administração Pública.

2. Constituir formalmente a Estrutura de Soberania Digital e Segurança da Informação (ESDSI), sob dependência direta do Governo, com competências em cibersegurança, gestão de informação classificada, resposta a incidentes e coordenação operacional da segurança digital do Estado. Esta estrutura integrará o CERT.PT e os centros nacionais de operações (SOC/NOC), assumindo as funções de CISO do Estado.

3. Desenvolver um Roteiro Nacional para a Cloud Soberana, com metas claras, prazos definidos e financiamento assegurado, integrando os investimentos previstos no PRR, PT2030 e fundos europeus para a transição digital. Este plano deverá incluir um calendário de adoção obrigatória e progressiva por toda a Administração Pública central e local, com apoio técnico e financeiro para a migração de serviços elegíveis.

4. Alinhar a execução da Cloud Soberana com a Estratégia Nacional de Soberania Digital e Segurança da Informação (ENDSI), garantindo coerência entre a arquitetura tecnológica, os mecanismos de governação, as normas de cibersegurança e a resiliência dos serviços públicos essenciais.

5. Reforçar e operacionalizar os mecanismos de governação estratégica, incluindo o Conselho para o Digital na Administração Pública (CDAP) como órgão consultivo ativo da AND, e consolidar o papel do Observatório de Cibersegurança do CNCS como instrumento técnico de acompanhamento da maturidade digital e da ciberresiliência da Administração Pública.

6. Mobilizar o ecossistema nacional de inovação, ciência e ensino, através de programas de capacitação para quadros públicos, parcerias com universidades,

colaboração com centros de investigação, e apoio à cocriação com startups e empresas tecnológicas. A Cloud Soberana deve ser também uma plataforma de inovação pública.

7. Colocar o cidadão no centro da estratégia digital do Estado, garantindo que os serviços públicos prestados através da Cloud Soberana sejam acessíveis, inclusivos, interoperáveis e baseados em dados com transparência, ética e respeito pelos direitos fundamentais.

Em síntese, a Cloud Soberana não é apenas uma solução tecnológica — é uma transformação estrutural e estratégica do Estado português, alicerçada na soberania digital, na modernização administrativa e na confiança institucional. O Observatório dos Ecossistemas e Infraestruturas Digitais (OEID) reafirma o seu compromisso com esta visão e disponibiliza-se para apoiar a sua concretização técnica, estratégica e política, em articulação com todos os atores públicos e privados relevantes.

Web Page: https://oeid.pt/

LinkedIn Page: linkedin.com/in/oeidobservatório