# DIÁRIO OFICIAL DA UNIÃO

Publicado em: 07/10/2026 | Edição: 190 | Seção: 1 | Página: 73

**Órgão: Ministério da Gestão e da Inovação em Serviços Públicos/Fundação Escola Nacional de Administração Pública**


CONSELHO DIRETOR

## RESOLUÇÃO ENAP Nº 101, DE 5 DE OUTUBRO DE 2026

Dispõe sobre a estratégia de uso de software e de serviços de computação em nuvem no âmbito da Fundação Escola Nacional de Administração Pública (Enap).

O CONSELHO DIRETOR DA FUNDAÇÃO ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA - ENAP, no uso das atribuições que lhe confere o art. 17, II, "a", do Estatuto aprovado pelo Decreto nº 10.369, de 22 de maio de 2020, considerando as exigências da Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023, e da Instrução Normativa GSI/PR n° 5/2021, e tendo em vista a deliberação do Comitê de Governança Digital (CGD/Enap) ocorrida entre 21 a 25 de setembro de 2026, conforme o Comunicado nº 6/2026/CGTI-CGD/CGTI/DGC, e o constante dos autos do processo nº 04600.003352/2025-75, resolve:

Art. 1° Fica aprovado, na forma do Anexo Único desta Resolução, o Documento de Estratégia de Uso de Software e de Serviços de Computação em Nuvem da Fundação Escola Nacional de Administração Pública (Enap), em conformidade com a Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023.

Art. 2° A Coordenação-Geral de Tecnologia da Informação (CGTI) da Enap deverá adotar, monitorar e garantir a aplicação das diretrizes estabelecidas na Estratégia de Uso de Software e de Serviços de Computação em Nuvem, visando garantir a qualidade e a conformidade na utilização dos recursos e nas contratações de software e dos serviços de nuvem de acordo com as necessidades de negócio do órgão.

Art. 3° Esta Resolução entrará em vigor na data de sua publicação.

**BETÂNIA LEMOS**

Presidenta do Conselho

ANEXO ÚNICODOCUMENTO ESTRATÉGIA DE USO DE SOFTWARE E DE SERVIÇOS DE COMPUTAÇÃO EM NUVEM

CAPÍTULO I

DISPOSIÇÕES GERAIS

Art. 1° Este documento estabelece a estratégia da Enap para o uso de software e serviços de computação em nuvem, visando orientar a contratação, adoção e gestão segura, eficiente e alinhada às diretrizes da transformação digital do Governo Federal.

Art. 2° Esta estratégia aplica-se a todas as contratações, implantações e operações de soluções que envolvam:

I - Software como Serviço (SaaS);

II - Infraestrutura como Serviço (IaaS);

III - Plataforma como Serviço (PaaS);

IV - Função como Serviço (FaaS);

V - Banco de Dados como Serviço (DBaaS);

VI - serviços de suporte técnico, migração, integração, operação e consultorias especializadas.

Art. 3° As áreas técnicas e administrativas da Enap, no planejamento e na execução de contratações e na gestão de soluções de tecnologia, devem observar as seguintes orientações:

I. avaliar a viabilidade de utilização de modelos já adotados na Administração, pois aumenta o nível de padronização nas contratações no âmbito do SISP;

II. não utilizar métrica de remuneração cuja medição não seja passível de verificação, nos termos da Súmula TCU 269;

III. avaliar a economicidade dos preços estimados e contratados, realizando a análise crítica da composição de preços unitários e do custo total estimado da contratação;

IV. abster-se de criar unidades de medida de forma unilateral, sem prévia avaliação técnica, econômica e de padronização;

V. não devem ser tratadas em ambiente de nuvem pública:

a) informações e cargas de trabalho que tratem informações classificadas em grau de sigilo (reservadas, secretas e ultrassecretas), nos termos do Decreto n.º 7.724, de 16 de maio de 2012; e

b) documentos preparatórios que possam originar informação classificada em grau de sigilo não devem ser tratadas em ambiente de nuvem público;

VI. dados tratados em ambiente de nuvem devem ser armazenados em data centers localizados em território brasileiro.

Parágrafo único. Admite-se o tratamento de dados em data centers fora do território brasileiro somente nos casos em que haja cópia de segurança atualizada armazenada em data centers localizados em território brasileiro, respeitando-se os demais limites estabelecidos neste modelo.

Art. 4° A adoção e o uso de software e serviços de computação em nuvem pela Enap pautar-se-ão pelos seguintes princípios:

alinhamento estratégico: as decisões sobre computação em nuvem devem estar alinhadas aos objetivos estratégicos da Enap e do Governo Federal, contribuindo para a modernização da gestão pública e a oferta de serviços de qualidade;

economicidade e eficiência: busca pela melhor relação custo-benefício, otimizando o uso de recursos públicos e aumentando a eficiência operacional, considerando o Custo Total de Propriedade (TCO);

Segurança da Informação e Privacidade: garantia da confidencialidade, integridade, disponibilidade e autenticidade das informações, segundo a Política Nacional de Segurança da Informação e a LGPD;

escalabilidade e flexibilidade: capacidade de ajustar os recursos de TIC conforme as necessidades da Enap, permitindo agilidade e adaptação a novas demandas;

inovação e modernização: fomento à adoção de tecnologias emergentes e soluções inovadoras que possam aprimorar os processos e serviços da Enap;

interoperabilidade e portabilidade: priorização de soluções que permitam a integração com sistemas legados e futuros, bem como a migração de dados e aplicações entre diferentes provedores ou ambientes, mitigando a dependência tecnológica (vendor lock-in);

sustentabilidade: consideração dos impactos ambientais e sociais na escolha e utilização de soluções de computação em nuvem;

transparência e controle: garantia de mecanismos de acompanhamento, auditoria e prestação de contas sobre o uso de software e serviços em nuvem;

foco no cidadão e no servidor público: utilização da tecnologia para melhorar a experiência dos usuários dos serviços da Enap, sejam eles cidadãos ou servidores públicos;

conformidade legal e regulatória: observância estrita da legislação e das normas aplicáveis às contratações públicas, à segurança da informação e à proteção de dados.

CAPÍTULO II

OBJETIVOS E COMPETÊNCIAS

Art. 5° Esta estratégia visa:

promover a transformação digital dos serviços e processos da Enap com apoio em soluções em nuvem seguras e eficientes;

garantir conformidade com os marcos legais de segurança da informação, proteção de dados e transparência pública;

otimizar o uso de recursos públicos com planejamento estratégico e governança;

assegurar resiliência, escalabilidade e continuidade dos serviços críticos da Enap;

orientar o planejamento de contratações para a melhor utilização dos recursos públicos.

Art. 6° A identificação do modelo de implantação de nuvem deve considerar as características de cada carga de trabalho em relação ao nível de sigilo das informações armazenadas ou manipuladas pelos serviços de Tecnologia da Informação e Comunicações (TIC) mantidos por essas cargas de trabalho.

Art. 7° Admite-se a utilização em ambiente de nuvem (pública, privada, híbrida, comunitária ou de governo) das cargas de trabalho que tratem informações sem restrição de acesso, considerada a legislação de dados pessoais e os aspectos de segurança da informação.

Art. 8° Devem ser mantidas em ambiente de nuvem de governo, exceto se expressamente determinado pelo Comitê de Governança Digital da Enap (mediante análise técnica fundamentada que justifique a segurança e a economicidade da decisão), cargas de trabalho que tratem informação com restrição de acesso prevista na legislação, a exemplo de: sigilo fiscal, bancário, comercial, empresarial, contábil, de segredo industrial, de direito autoral, de propriedade intelectual, industrial, policial, processual civil, processual penal e disciplinar administrativa.

CAPÍTULO II - SEÇÃO I

Da Alta Administração

Art. 9° Compete à alta administração da Enap, com apoio da área de tecnologia da informação:

I - aprovar e garantir os recursos necessários para a implementação desta estratégia;

II - promover a cultura de uso seguro e eficiente da computação em nuvem na instituição;

III - tomar decisões estratégicas relativas à adoção de nuvem, com base nas recomendações técnicas e de governança.

CAPÍTULO II - SEÇÃO II

Do Comitê de Governança Digital (CGD/Enap)

Art. 10. Compete à alta administração da Enap, com apoio da área de tecnologia da informação:

I - deliberar sobre as políticas, normas e planos relacionados à computação em nuvem;

II - acompanhar a implementação desta estratégia e avaliar seus resultados;

III - arbitrar sobre casos omissos ou conflitos de interpretação desta estratégia.

CAPÍTULO II - SEÇÃO III

Da Coordenação-Geral de Tecnologia da Informação (CGTI)

Art. 11. Compete à Coordenação-Geral de Tecnologia da Informação (CGTI):

propor, implementar e gerenciar as soluções de software e serviços em nuvem, conforme esta estratégia;

prestar suporte técnico e orientação às áreas de negócio quanto ao uso de soluções em nuvem;

gerenciar os contratos com os provedores de serviços em nuvem;

monitorar a segurança, o desempenho e os custos dos serviços em nuvem;

manter-se atualizada sobre as novas tecnologias e melhores práticas em computação em nuvem.

CAPÍTULO II - SEÇÃO IV

Do Gestor de Segurança da Informação

Art. 12. Compete ao Gestor de Segurança da Informação:

I - definir e fiscalizar o cumprimento dos requisitos de segurança para soluções em nuvem;

II - realizar análises de risco e propor medidas mitigatórias;

III - gerenciar incidentes de segurança relacionados a serviços em nuvem;

IV - promover a conscientização sobre segurança da informação no contexto da nuvem.

CAPÍTULO II - SEÇÃO V

Das Áreas de Negócio

Art. 13. Compete às áreas de negócio (Diretorias, Coordenações e demais unidades demandantes):

I - identificar as necessidades de negócio que podem ser atendidas por soluções em nuvem;

II - participar da especificação e validação das soluções em nuvem;

III - utilizar as soluções em nuvem de forma segura e segundo as políticas da Enap.

CAPÍTULO II - SEÇÃO VI

Do Encarregado pelo Tratamento de Dados Pessoais (DPO)

Art. 14. Compete ao Encarregado pelo Tratamento de Dados Pessoais (DPO):

I - orientar e fiscalizar a conformidade das soluções em nuvem com a LGPD;

II - participar da avaliação de impacto à proteção de dados (DPIA) para novas soluções em nuvem.

CAPÍTULO III

DIRETRIZES PARA DEFINIÇÃO DA ESTRATÉGIA

Art. 15. A Enap adota as seguintes diretrizes para orientar o uso de software e serviços de computação em nuvem, de forma a garantir segurança, eficiência, governança e alinhamento estratégico com as políticas públicas:

I - identificação das necessidades do negócio - todas as iniciativas em nuvem deverão partir da análise das necessidades específicas das áreas de negócio da Enap, considerando:

a) os serviços, sistemas, dados e aplicações que demandam escalabilidade ou alta disponibilidade;

b) a natureza dos dados (abertos, pessoais, sensíveis, sigilosos ou classificados);

c) os requisitos de desempenho, acessibilidade e continuidade.

II - seleção dos modelos adequados (IaaS, PaaS, SaaS, nuvem pública, híbrida, privada ou de governo) - a escolha do modelo de serviço e de implantação será pautada em:

a) maturidade técnica da Enap para operar e governar o serviço;

b) natureza dos dados a serem tratados;

c) critérios de custo-benefício, agilidade e segurança;

d) a abordagem cloud híbrida será preferencial, permitindo combinar controle e escalabilidade, dados com restrição de acesso serão priorizados em nuvem de governo ou ambiente controlado.

III - avaliação dos possíveis fornecedores - as contratações serão precedidas de estudo técnico com análise de fornecedores com:

experiência comprovada em ambientes governamentais;

certificações de conformidade e segurança (ex.: ISO/IEC 27001, SOC 2 tipo II);

capacidade técnica, suporte local, Acordo de Nível de Serviço (ANS) compatível com as exigências institucionais;

o princípio da economicidade e da pluralidade de fornecedores será respeitado.

IV - definição dos requisitos mínimos obrigatórios de segurança, incluindo:

a) criptografia ponta a ponta;

b) autenticação multifator (MFA);

c) segmentação de redes;

d) gestão de identidade e acesso com privilégios mínimos;

e) registro e auditoria de logs.

V - estabelecimento de uma política de governança em nuvem envolverá:

a) controle de acesso baseado em função (RBAC);

b) classificação da informação conforme o Decreto nº 7.724/2012;

c) monitoramento contínuo;

d) conformidade com a Política de Segurança da Informação da Enap;

e) acompanhamento pelo Comitê de Governança Digital.

somente poderão ser migrados à nuvem os dados e sistemas cuja análise de impacto e classificação permitam. Será exigida mitigação de riscos por meio de:

a) controles técnicos e administrativos;

b) treinamento de usuários;

c) planos de resposta a incidentes;

d) respeito à LGPD e demais normativos;

e) ambientes em nuvem pública não poderão processar informações classificadas (reservadas, secretas ou ultrassecretas).

antes da adoção de serviços em nuvem, será avaliada a infraestrutura de TIC da Enap quanto a:

a) conectividade (banda larga estável e segura);

b) capacidade da equipe técnica;

c) ferramentas de gestão e monitoramento existentes.

papéis e responsabilidades na governança dos contratos de nuvem:

a) área de TIC: planejamento, execução e fiscalização contratual;

b) áreas de negócio: levantamento das necessidades e validação das entregas;

c) Comitê de Governança Digital: priorização, monitoramento e deliberação estratégica.

princípios norteadores da estratégia

a) cloud smart (adoção estratégica, segura e eficiente);

b) interoperabilidade entre sistemas e dados;

c) resiliência e disponibilidade contínua;

d) lift-and-shift como exceção, preferindo reengenharia e modernização;

e) uso de cloud broker quando necessário, com foco em portabilidade e conformidade.

todas as iniciativas dessa estratégia deverão ser alinhadas aos seguintes instrumentos:

a) Plano Estratégico Institucional (PEI);

b) Plano Diretor de TIC (PDTIC);

c) Plano de Contratações Anual (PCA);

d) Plano de Segurança da Informação;

e) Política de Proteção de Dados Pessoais.

cada iniciativa deverá conter mapeamento AS IS (estado atual) e definição do TO BE (estado desejado), com indicadores como:

a) tempo médio de provisionamento;

b) redução de custos operacionais;

c) aumento de disponibilidade e desempenho;

d) nível de satisfação do usuário;

e) conformidade com LGPD e políticas de segurança.

a Enap promoverá a capacitação contínua dos servidores envolvidos com a gestão, operação e uso de soluções em nuvem, priorizando:

a) segurança da informação;

b) gerenciamento de contratos e custos;

c) arquitetura e engenharia de nuvem;

d) ferramentas de monitoramento e automação.

serão observados requisitos de interoperabilidade entre plataformas, serviços e bases de dados, visando evitar dependência de fornecedor (vendor lock-in), os contratos incluirão cláusulas de portabilidade, formatos abertos e APIs padronizadas.

requisitos regulatórios e de conformidade:

a) LGPD (Lei nº 13.709/2018);

b) Lei de Acesso à Informação (Lei nº 12.527/2011);

c) Marco Civil da Internet (Lei nº 12.965/2014);

d) normas técnicas de segurança da informação e privacidade (ISO/IEC 27001, 27701 etc.);

e) normas do TCU e CGU aplicáveis à contratação pública.

definição da Estratégia de saída, ou seja, cada contrato de serviços em nuvem conterá cláusula de saída que inclua:

a) plano de migração reversa para infraestrutura local ou outro provedor;

b) backup completo e atualizado;

c) devolução segura dos dados;

d) suporte na transição durante período definido;

e) garantia de portabilidade dos dados em formato aberto.

toda iniciativa em nuvem será acompanhada por um plano de gerenciamento de riscos com:

a) mapa de riscos atualizado;

b) análise de impacto (BIA - Business Impact Analysis);

c) estratégias de mitigação, aceitação ou transferência;

d) monitoramento contínuo dos riscos residuais;

e) registro em ferramenta oficial da Enap.

Parágrafo único. O mapeamento de que trata o caput será consolidado nos documentos de planejamento da contratação (Estudo Técnico Preliminar - ETP e Termo de Referência - TR) e vinculado ao Plano Diretor de TIC (PDTIC).

CAPÍTULO IV

DEFINIÇÃO DOS REQUISITOS DE SEGURANÇA

Art. 16. A Enap adota os seguintes requisitos técnicos e normativos para garantir a segurança, resiliência e conformidade no uso de serviços de computação em nuvem, em alinhamento com a Instrução Normativa GSI/PR nº 5/2021, Portaria SGD/MGI nº 5.950/2023 e a legislação vigente:

I - toda informação deve ser previamente classificada conforme a Tabela de Classificação da Informação da ENAP, com base no Decreto nº 7.724/2012 e na Lei nº 12.527/2011 (Lei de Acesso à Informação);

II - informações com restrição de acesso (ex.: dados pessoais sensíveis, informações fiscais, processuais, de pesquisa sigilosa etc.) só poderão ser processadas em nuvem governamental, privada ou comunitária, com controle total da ENAP ou de ente público responsável;

III - as soluções em nuvem devem oferecer mecanismos de segurança:

a) criptografia de dados em trânsito e em repouso com algoritmos aderentes aos padrões do GSI/PR;

b) controle de acesso baseado em identidade (IAM), com autenticação multifator (MFA) obrigatória;

c) segmentação lógica e física de ambientes, com políticas claras de isolamento entre tenants (instâncias ou ambientes em nuvem);

d) rastreamento de atividades e trilhas de auditoria com retenção mínima legal;

e) resiliência e alta disponibilidade, com garantias contratuais de continuidade de serviço (recuperação de desastres e failover (redundância));

f) atualizações e correções de segurança automatizadas, auditáveis e gerenciadas com base em ciclos regulares.

IV - os dados deverão ser armazenados preferencialmente em data centers localizados em território nacional. Casos excepcionais de uso de data centers fora do país só serão aceitos com:

a) cópia de segurança (backup) atualizada e integral mantida em território brasileiro;

b) avaliação formal do Comitê de Governança Digital da ENAP;

c) garantia contratual da soberania jurídica sobre os dados.

V - todos os contratos com provedores de nuvem deverão prever cláusulas específicas sobre relatórios e auditoria:

a) garantia de confidencialidade, integridade e disponibilidade da informação;

b) responsabilidade solidária do cloud broker, quando houver;

c) apresentação obrigatória dos relatórios de auditoria SOC 2 tipo II, ISO/IEC 27001 ou equivalente;

d) permissão para auditoria externa ou interna por parte da ENAP, órgãos de controle ou parceiros credenciados.

VI - requisitos de Governança e Gestão de Riscos:

Mapa de riscos para serviços em nuvem, com análise de probabilidade, impacto e plano de tratamento;

Plano de continuidade de negócios (PCN) específico para cargas de trabalho em nuvem;

Plano de saída (estratégia de exit) com procedimentos para portabilidade, migração reversa, destruição segura de dados e mitigação de aprisionamento tecnológico (vendor lock-in);

diretrizes para controle de consumo e alocação de recursos computacionais.

VII - capacitação e conscientização:

a) capacitação técnica da equipe de TIC, segurança da informação e áreas usuárias;

b) conscientização institucional sobre riscos e boas práticas no uso da nuvem;

c) atualização normativa sobre segurança da informação e proteção de dados.

CAPÍTULO V

DISPOSIÇÕES FINAIS

Art. 17. Esta estratégia bem como os documentos gerados a partir dela devem ser revisados, aprovados e atualizados em função de alterações na legislação pertinente, de diretrizes políticas do governo federal, de alterações nas políticas e normas da Enap, quando considerada necessária pelo Comitê de Segurança da Informação.

Art. 18. Em função da capacidade de os provedores de serviço de computação em nuvem implementar atualizações relacionadas à segurança da informação em seus produtos e serviços, a presente estratégia deve ser revisada em até 2 (dois) anos para:

I - definir novos critérios e a periodicidade das atualizações dos procedimentos e dos recursos computacionais a serem observados pelo provedor de serviço de nuvem;

II - atualizar periodicamente os processos internos de gestão de riscos de segurança da informação.

Parágrafo único. A estratégia também será revisada quando ocorrerem eventos, fatores relevantes, novos requisitos tecnológicos, corporativos e/ou legais que exijam sua revisão imediata.

Art. 19. As novas contratações de software e serviços de computação em nuvem devem observar as diretrizes apresentadas neste documento, bem como o modelo de contratação de software e de serviços de computação em nuvem, no âmbito dos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

Art. 20. Esta estratégia e seus documentos complementares devem ser divulgados a todos os usuários e partes interessadas, mediante publicação no Boletim de Serviço Eletrônico e no portal da Enap na internet, a fim de promover sua observância e conhecimento.

Art. 21. A alta administração deve priorizar a alocação dos recursos (humanos, tecnológicos e financeiros) necessários para a execução desta estratégia.

Art. 22. Os casos omissos e os conflitos de interpretação não abordados neste documento serão analisados pelo Comitê de Governança Digital.

Este conteúdo não substitui o publicado na versão certificada.