

# O avanço da soberania nos governos globais

## O caminho para a sobrevivência no setor público

Para órgãos públicos fora dos Estados Unidos, a soberania digital deixou de ser um mero item de conformidade e se tornou uma estratégia de sobrevivência. Os governos agora percebem que a soberania ou a conformidade com as leis locais, isoladamente, já não são suficientes. O novo objetivo da soberania digital é conhecido como autonomia estratégica: a capacidade de operar, inovar e manter serviços críticos de forma independente, mesmo quando o suporte externo deixa de existir ou as cadeias globais de suprimentos são interrompidas.

Um relatório recente da Conferência das Nações Unidas sobre Comércio e Desenvolvimento (UNCTAD) afirmou que "79% dos países com legislação de privacidade e proteção de dados estão preocupados com a soberania digital".<sup>1</sup> Os governos não podem mais ignorar as dependências inerentes aos sistemas proprietários fechados. Três fatores influenciam a transformação para a autonomia estratégica:

- ▶ **Risco geopolítico:** em períodos de estabilidade, controlar a dependência de hyperscalers globais é uma tarefa viável. No entanto, em cenários de conflito, a dependência do suporte externo se torna uma vulnerabilidade crítica. A destruição física ou interrupções na internet paralisam as operações dependentes da nuvem. É fundamental que as nações tenham a autonomia para agir de forma independente caso a cooperação internacional falhe ou se torne instável. Para isso, são necessários sistemas aptos a funcionar em condições de conectividade intermitente ou limitada (DDIL). Assim, as funções essenciais à missão (como sistemas de comando e controle de defesa e serviços ao atendimento emergencial à população) continuam ativas mesmo em caso de desconexão total da internet global.
- ▶ **Resiliência cibernética:** os ciberataques patrocinados por Estados estão cada vez mais sofisticados, frequentes e influentes. A soberania garante que infraestruturas críticas, como redes de energia, sistemas de saúde e de defesa, permaneçam resilientes contra interferências externas e sabotagens na cadeia de suprimentos. O risco inclui roubo de dados e a inserção de códigos maliciosos em atualizações de software em trânsito. Os governos exigem garantias de soberania: a capacidade de verificar, de forma independente, a integridade de sua cadeia de suprimentos de software para evitar espionagem estrangeira e assegurar que os sistemas não foram comprometidos.
- ▶ **Competitividade econômica:** cada vez mais, os governos veem a soberania digital como um dos pilares da segurança nacional. Ao manter o desenvolvimento da IA e a governança de dados em âmbito local, os pilares do crescimento econômico futuro permanecem sob jurisdição doméstica, evitando a supervisão estrangeira. Há uma preocupação crescente de que a dependência de modelos de IA de caixa preta de outros países leve à perda de propriedade intelectual e de relevância cultural. Com a autonomia estratégica, as nações desenvolvem essas capacidades digitais, promovendo ecossistemas locais de inovação e garantindo que o valor econômico gerado pela transformação digital permaneça na economia nacional.

<sup>1</sup> ["Data protection and privacy legislation worldwide"](#), UNCTAD, 17 de fevereiro de 2026.

## **Demanda global e realidade regional**

A demanda por controle é global, mas as influências e barreiras específicas que o setor público enfrenta variam conforme a região.

### **Europa, Oriente Médio e África (EMEA)**

Na região EMEA, o principal problema é precisar de tecnologia avançada e, ao mesmo tempo, depender de provedores de fora da União Europeia (UE). Isso expõe os governos a riscos jurídicos, especificamente leis extraterritoriais como as aprovadas pelos Estados Unidos, incluindo a Lei para Esclarecer o Uso Legal de Dados no Exterior ([CLOUD](#)) ou Lei de Vigilância de Inteligência Estrangeira de 1978 ([FISA](#)).

Os órgãos europeus enfrentam uma complexa rede de regulamentações rigorosas, incluindo o [NIS2](#) da UE para cibersegurança e o Regulamento de Resiliência Operacional Digital (DORA), além de [legislações nacionais](#) como o SecNumCloud da França. A infraestrutura de defesa continua fragmentada, com lacunas de interoperabilidade na Organização do Tratado do Atlântico Norte (OTAN) atrasando a troca de dados. Além disso, os países enfrentam uma escassez crítica de funcionários com certificação de segurança para operar ambientes soberanos. O Canadá, apesar de ficar na região da América do Norte, têm os mesmos desafios que a EMEA em relação à infraestrutura desatualizada. O Departamento de Defesa Nacional do Canadá enfrenta desafios com uma infraestrutura de rede secreta consolidada (CSNI) fragmentada, além de entraves burocráticos que retardam a adoção de recursos modernos. Por causa do risco, as agências governamentais protegem dados confidenciais de interferências jurídicas estrangeiras e desenvolvem capacidade interna para suprir a falta de software.

### **Ásia-Pacífico (APAC)**

A região da APAC conta com legislações protecionistas rigorosas e conformidade de alto risco para alcançar a autossuficiência tecnológica.

- ▶ **Localização dos dados:** países como a China, a Índia e a Indonésia impõem regras rígidas de localização de dados, exigindo que os dados críticos residam dentro das fronteiras nacionais, limitando o uso de nuvens públicas globais.
- ▶ **Alta responsabilização:** em Singapura, o rigor dos padrões de segurança de ponta a ponta prevê sanções criminais para funcionários que utilizem ou extraviem dados indevidamente. Esse cenário consolida uma cultura de aquisição extremamente avessa ao risco.
- ▶ **Requisitos globais e locais:** há uma forte preferência por modelos globais e locais (glocal), parcerias nas quais a tecnologia global é entregue por empresas locais para garantir controle soberano.

O foco da região APAC é desenvolver competências nativas para diminuir a dependência estrutural de potências estrangeiras, utilizando a soberania digital como proteção de incertezas geopolíticas.

### **América Latina (LATAM)**

A modernização na região LATAM é influenciada pela continuidade operacional e, muitas vezes, é prejudicada pela instabilidade estrutural, e não pelas políticas.

- ▶ **Instabilidade e descontinuidade:** mudanças frequentes na liderança política e volatilidade econômica colocam em risco o planejamento da TI a longo prazo, comprometendo contratos de aquisição de vários anos em um clima geopolítico incerto.

- ▶ **Foco na segurança interna:** na América Latina, as agências de defesa priorizam a segurança interna (como o controle de fronteiras e o combate ao narcotráfico), privilegiando ferramentas de vigilância ágeis em detrimento de uma infraestrutura estratégica pesada.<sup>2</sup>
- ▶ **Riscos de aquisição:** as ineficiências e os riscos de corrupção nas aquisições públicas reduzem o valor real dos orçamentos de tecnologia. Isso gera a demanda por sistemas econômicos, abertos e flexíveis, capazes de resistir a cortes orçamentários e trocas de governo sem aprisionar o país a fornecedores proprietários rígidos e onerosos.

### A abordagem da Red Hat para a soberania digital

Para ter sucesso, os órgãos públicos globais precisam abordar a soberania sob diferentes dimensões. A Red Hat oferece as ferramentas e o ecossistema necessários para gerir cada uma delas.

#### Soberania de dados e IA

A Red Hat viabiliza o controle e a autonomia total sobre dados críticos e modelos de IA, assegurando a residência das informações em território nacional e uma governança alinhada às leis locais. É fundamental que as agências adotem estratégias de IA soberana para manter o controle sobre modelos e bases de treinamento. Isso exige a execução em infraestrutura própria, em vez de depender do acesso via API a modelos controlados por entidades estrangeiras. O Red Hat® OpenShift® AI permite a implantação de recursos de IA soberana onde os dados residem. Viabilizamos o controle sobre a localização e o acesso aos dados por meio da computação confidencial, que protege as informações durante o uso e assegura a conformidade com regulamentações como a Lei de IA da UE.

#### Soberania tecnológica

Para garantir independência no longo prazo e a liberdade de mover aplicações sem restrições, é essencial conseguir executar cargas de trabalho sem depender da infraestrutura de um provedor específico ou de software proprietário. Os governos devem evitar a dependência de fornecedor, adotando padrões abertos e plataformas de containers portáteis. Se as políticas de um provedor de nuvem mudarem ou as tensões geopolíticas aumentarem, é possível migrar as cargas de trabalho para outra infraestrutura sem refatoração. A Red Hat reduz a dependência de fornecedor por meio de padrões open source. Nossa plataforma é compatível com várias arquiteturas de hardware, como x86, Advanced RISC Machine (ARM) e RISC-V. Assim, os sistemas nacionais podem evoluir e ser atualizados no próprio ritmo, independentemente das dependências externas.

#### Soberania operacional

Os órgãos governamentais precisam manter controle total e autonomia sobre suas operações críticas de TI para continuar funcionando mesmo quando estiverem desconectados. A defesa e a infraestrutura crítica devem priorizar a resiliência operacional. Essa infraestrutura envolve automatizar planos de recuperação de desastres que considerem condições de guerra e garantir que o suporte e as operações sejam conduzidos por cidadãos locais com credenciais de segurança. Por exemplo, a Red Hat oferece suporte soberano verificado: atendimento técnico realizado por cidadãos locais credenciados (como na União Europeia), garantindo que nenhum dado acessado pela equipe saia da jurisdição. Além disso, o Red Hat Ansible® Automation Platform automatiza a resiliência, viabilizando a recuperação ágil e atualização por patches mesmo em ambientes desconectados (DDIL).

#### Soberania de confiabilidade

A verificação independente da integridade, da segurança e da confiabilidade de sistemas e processos digitais ajuda os órgãos a manter a conformidade. Não dá para confiar sem verificar: as agências precisam de uma confiança verificável. Essa mudança exige uma auditoria rigorosa da cadeia de suprimentos de software e a capacidade de comprovar conformidade com padrões como Common Criteria, Federal Information Processing Standards (FIPS) e NIS2. A Red Hat oferece uma cadeia de

---

2 ["New Pentagon strategy to focus on homeland, Western Hemisphere"](#), DefenseNews, 25 de setembro de 2025.

suprimentos de software confiável, oferecendo software assinado por criptografia com procedência verificada e uma lista de materiais (SBOM). Isso permite que os órgãos auditem cada componente e assegurem a ausência de código malicioso. Com essas medidas de segurança, é possível verificar se os órgãos estão cumprindo as novas exigências, como a Lei de Resiliência Cibernética da União Europeia.

### **Autonomia estratégica com o open source**

A Red Hat usa uma base aberta e flexível para responder aos desafios, dando aos órgãos governamentais mais opções e controle, em vez de isolamentos rígidos. Essa abordagem flexível reconhece que um único provedor raramente resolve a questão da soberania digital. A Red Hat oferece a opção de desenvolver uma nuvem soberana em vários provedores de infraestrutura e zonas de nuvem, evitando as limitações de uma única solução.

Há mais de 30 anos, a Red Hat fornece soluções open source empresariais confiáveis para organizações com os mais rigorosos requisitos de segurança e conformidade. O open source empresarial vai além da tecnologia: ele é uma base arquitetônica essencial para os órgãos governamentais conquistarem a verdadeira soberania digital e autonomia estratégica. Diferentemente de fornecedores proprietários que contam com sistemas fechados e pouco transparentes e exigem confiança cega, a Red Hat ajuda os órgãos a manter controle absoluto sobre seu destino digital em vez de depender de terceiros. Essa abordagem aberta ajuda o setor público ao redor do mundo a ditar o ritmo da inovação, da edge táctica da rede à IA soberana, garantindo que as cargas de trabalho permaneçam portáteis e resilientes. Uma abordagem open source também protege as operações de importância crítica dos riscos de dependência de fornecedores e da obsolescência tecnológica. Ao usar a tecnologia open source, a Red Hat se alinha a uma filosofia open source que prevalece em regiões como a União Europeia. Usar um modelo como esse evita a dependência de um único fornecedor e permite a inspeção e modificação do código, essencial para a segurança e a confiança nacionais.

#### ▶ **Transparência e confiança**

O modelo open source da Red Hat oferece transparência total, permitindo que órgãos governamentais inspecionem o código-fonte, verifiquem a segurança e auditem as cadeias de suprimentos de software. Essa capacidade de auditoria é essencial para cumprir os requisitos de garantia nas regiões EMEA e APAC. Além disso, a Red Hat oferece software com assinatura criptográfica com procedência verificada para atender a novas exigências, como a [Lei de Resiliência Cibernética da EU](#).

#### ▶ **Soberania das operações e suporte local**

Para lidar com os riscos jurisdicionais, a Red Hat permite controlar quem opera a infraestrutura, assegurando a soberania operacional.

- ▶ **Suporte soberano:** como já mencionado, a Red Hat oferece suporte soberano verificado na União Europeia, com atendimento técnico prestado exclusivamente por cidadãos do bloco, localizados na região. Esse modelo de suporte ajuda a assegurar que nenhum dado acessado pela equipe deixe a região.
- ▶ **Ecossistemas locais:** um ecossistema de parceiros da Red Hat com provedores de nuvem locais e certificados está disponível para oferecer recursos de nuvem soberana que atendem às rigorosas leis de residência nacional.

#### ▶ **Independência tecnológica**

Uma estratégia de nuvem híbrida aberta permite que as cargas de trabalho sejam executadas em vários ambientes, como on-premise, em uma nuvem privada, na edge da rede táctica ou em um ambiente isolado.

- ▶ **Portabilidade:** essa é a base para evitar a dependência de fornecedor, uma preocupação primordial para órgãos governamentais, especialmente em regiões como LATAM e APAC. A capacidade de essas regiões migrarem cargas de trabalho e dados com eficiência é essencial para garantir a continuidade dos serviços e responder rapidamente a mudanças geopolíticas, como alterações políticas ou econômicas que exijam a troca de provedores de tecnologia.
- ▶ **Operações desconectadas:** para os órgãos de defesa, as soluções da Red Hat, como o Red Hat Device Edge e o Red Hat OpenShift, permitem que os sistemas operem de forma autônoma em ambientes DDIL, garantindo a continuidade da missão mesmo quando a nuvem central estiver inacessível.

A Red Hat oferece aos órgãos governamentais a base open source para desenvolver uma nuvem soberana que sobrevive à incerteza, oferece segurança de dados confiável e mantém um país funcionando.

#### ▶ IA soberana

Conforme os governos exploram e expandem a IA, a Red Hat fornece a plataforma para desenvolver uma IA soberana. Isso permite que os países mantenham a propriedade de seus modelos e dados de treinamento ao implantá-los em infraestrutura local, em conformidade com Lei de IA da UE, em vez de depender do acesso via API a modelos sob controle estrangeiro.

### Por escolher a Red Hat para o setor público?

A Red Hat tem sido uma parceira de confiança do setor público, com soluções implantadas em todos os departamentos executivos dos EUA<sup>3</sup> e amplamente usada na OTAN e em ministérios da defesa do mundo todo. O modelo de licenciamento da Red Hat e o compromisso com os padrões abertos asseguram que esses órgãos nunca fiquem dependentes de um fornecedor para sempre. As organizações têm o direito de usar e manter o software por tempo indeterminado, protegendo investimentos de longo prazo contra mudanças nos roadmaps de fornecedores ou restrições geopolíticas.

Com o aumento dos gastos, sobretudo no setor de defesa, o investimento no portfólio de soluções e serviços da Red Hat tende a proporcionar um retorno sobre o investimento mensurável. Os gastos comprometidos dos países membros da [OTAN](#) devem dobrar, chegando a 5% do Produto Interno Bruto (PIB) nacional até 2035.<sup>4</sup> Ao padronizar uma plataforma unificada, os órgãos podem direcionar recursos antes gastos na manutenção de sistemas convencionais e fragmentados para desenvolver novas capacidades de missão, reduzindo bastante os custos operacionais e o custo total de propriedade.

### Próximas etapas para começar

- ▶ Descubra mais informações sobre a [Red Hat no setor público global](#) e fale com um consultor da Red Hat.
- ▶ Quer avaliar se sua empresa está pronta para a soberania digital? [Leia este artigo do blog](#) para começar.



#### Sobre a Red Hat

A Red Hat é a líder mundial em soluções de software open source empresarial e utiliza uma abordagem impulsionada pela comunidade para oferecer tecnologias confiáveis e de alto desempenho em Linux, nuvem híbrida, containers e Kubernetes. A Red Hat ajuda os clientes a desenvolver aplicações nativas em nuvem, integrar aplicações de TI novas e existentes e automatizar e gerenciar ambientes complexos. [Parceira de confiança das empresas da Fortune 500](#), a Red Hat oferece serviços de consultoria, treinamento e suporte [premiados](#), compartilhando os benefícios da inovação open source com todos os setores. A Red Hat é um hub que conecta uma rede global de empresas, parceiros e comunidades, ajudando organizações a crescer, se transformar e se preparar para o futuro digital.

3 Dados de clientes da Red Hat, setembro de 2025.

4 "[Defence expenditures and NATO's 5% commitment](#)", OTAN, 18 de dezembro de 2025.