IV CONGRESSO DE DIREITO TRIBUTÁRIO E ADUANEIRO DA RECEITA FEDERAL

Tributação, Inteligência e Justiça Fiscal

Soberania digital na era da IA: O Estado em um mundo interdependente

André Molina

Secretário de Segurança da Informação e Cibernética do GSI/PR

Outubro de 2026

Quando dados, modelos de IA, infraestrutura computacional e nuvem se tornam ativos estratégicos, o que significa soberania digital para o Estado brasileiro?

A informação em um mundo interdependente

O problema contemporâneo não é depender. É depender sem conhecer, sem alternativa e sem capacidade de gestão e decisão.

Inteligência artificial

Modelos, dados e inferência

Nuvem

Processamento e armazenamento

Software

Camadas invisíveis de dependência

Semicondutores

Produção concentrada em poucos países

Telecom

Conectividade e operação em diferentes jurisdições

Cabos submarinos

Fluxo internacional de dados

Satélites

Comunicação e observação

Plataformas digitais

Intermediação e governança privada

Interdependência não elimina soberania.
Dependência não gerenciada pode restringir a soberania.

Três dependências que viraram interrupção

Serviços desabilitados por decisão da empresa, após revisão interna concluir que o uso violava seus termos de serviço.

Instabilidades em ambientes de nuvem causaram a interrupção de milhares de empresas no mundo, incluídos serviços essenciais e infraestruturas críticas.

Por 19 dias, o Claude Fable 5 e Mythos ficaram fora do ar no mundo inteiro por regra de controle de exportação dos Estados Unidos.



Mundo | Oriente Médio

Microsoft corta acesso do Exército de Israel a serviços de nuvem e IA

Decisão ocorre após revelações de que unidade militar usava Azure para vigiar palestinos

Marina Verenicz Seguir

25/09/2025 18h53 • Atualizado 1 ano atrás



AWS e Cloudflare: por que apagões na internet global estão mais comuns?

Falha na Cloudflare não é o primeiro 'apagão' de internet este ano

Vitoria Lopes Gomez

18/11/2025 12:59, atualizada em 18/11/2025 21:27



EUA suspendem controle de exportação de modelos de IA da Anthropic

Ordem de 12 de junho que exigia que a Anthropic restringisse imediatamente o acesso ao Mythos 5 e ao Fable 5 para cidadãos estrangeiros levou a empresa a desativar ambos os modelos para todos os usuários

Por Reuters — São Paulo

01/07/2026 08h56 · Atualizado 04/07/2026 22h10

Uma dependência relevante não precisa estar em um adversário

A informação é o ativo a proteger

Ela só sustenta a soberania quando permanece confiável.

SEGURANÇA DA INFORMAÇÃO

É o conjunto de ações destinadas assegurar a **disponibilidade**, a **integridade**, **confidencialidade** e **autenticidade**, abrangendo a segurança dos dados, dos ativos de informação, dos processos organizacionais, do ambiente físico e eletrônico em que tais ativos são tratados e do pessoal envolvido no ciclo de vida da informação.



Pessoas

comportamento, liderança e cultura



Processos

regras, governança e responsabilidades



Ambiente físico

controle de acesso e proteção de instalações



Tecnologia

sistemas, redes e arquitetura



Informação

o ativo que precisa permanecer confiável



Cibersegurança: dimensão do ambiente digital

O que é soberania digital

É o poder de entender e decidir sobre a cadeia de valor digital (os dados e as tecnologias de que depende), e de continuar funcionando e decidindo mesmo com fatores externos.

Controle

Saber onde estão os dados, quem os acessa e sob qual lei

Autonomia

Ter alternativas de fornecedores ou países

Resiliência

Seguir funcionando mesmo sob crise ou pressão externa

Não é autossuficiência. É ter capacidade de escolher consciente.

O problema não é depender. É depender sem conhecer, sem alternativa e sem capacidade de decidir.

Avaliação de Autonomia Tecnológica: CTS-FGV

1 Independência jurídica e estrutural

ETAPA INICIAL

O fornecedor está livre de coerção por ordenamento estrangeiro?
Avalia a profundidade da cadeia societária, o local de incorporação e as legislações a que seus controladores se submetem.

2 Robustez da cadeia de suprimentos

Dependência de componentes críticos vindos de jurisdições instáveis. Exige plano formal e auditável de contingência.

3 Localização de categorias de dados

Informações estratégicas ou classificadas tratadas e administradas no país. Categorias específicas, não todo dado.

4 Autonomia da equipe técnica

Quem tem acesso privilegiado reside no país, é contratado por empresa nacional e opera a partir do território.

5 Interoperabilidade e portabilidade

Padrões abertos, APIs documentadas e liberdade de migrar. Padrões fechados devem ser restringidos.

6 Arquiteturas abertas e auditáveis

Auditoria independente possível: acesso ao código e documentação da lógica interna. Sem isso, não se qualifica.

7 Reversibilidade e continuidade

A administração consegue assumir ou transferir a operação em caso de falha, interrupção ou fim de contrato.

BELLI, L. et al. Soberania Digital e Inteligência Artificial no Brasil. CTS-FGV / CyberBRICS. Rio de Janeiro: Lumen Juris, 2026, p. 212-214.

Cada nação desenvolve seu conceito

Políticas de soberania digital são moldadas por agendas domésticas, prioridades e interesses.

Estados Unidos

EIXO

Autorregulação corporativa, com foco em segurança nacional

MECANISMO

Fluxo livre de dados, sem lei federal geral de proteção de dados, alcance extraterritorial sobre dados sob custódia de empresas do país

China

EIXO

Controle estatal do domínio digital

MECANISMO

Tripé legal de cibersegurança, segurança de dados e proteção de informações pessoais; localização para infraestrutura crítica; avaliação prévia de transferências

União Europeia

EIXO

Proteção de direitos individuais e privacidade

MECANISMO

RGPD com aplicação extraterritorial, transferências condicionadas a salvaguardas, ambição de definir normas globais

E o Brasil? LGPD de inspiração europeia, Marco Civil, autonomia tecnológica como objetivo constitucional, regras esparsas. A composição ainda é escolha em aberto.

Soberania digital não é um conceito único. Cada país o preenche conforme sua agenda doméstica.

MUSONI, M. et al. Global approaches to digital sovereignty. ECDPM Discussion Paper 344, 2023.

Soberania digital no Brasil: exemplo da computação em nuvem

O Brasil regula computação em nuvem de forma fragmentada, sem uma lei única, mas com um conjunto coerente de normas

/NÃO EXAUSTIVO /PRELIMINAR

Leis gerais que impactam *Cloud*

LGPD (Lei 13.709/2018)

Exige base legal, contrato com operador, segurança, limites à transferência internacional e reporte de incidentes (Fiscalização ANPD)

Marco Civil da Internet (Lei 12.965/2014)

Fixa privacidade, neutralidade e guarda de registros, com acesso a dados só por ordem judicial

Regulação de *Cloud* para setor público

Leis

- **Lei de Acesso à informação (Lei 12.527/2011):** impõe transparência e acesso, com classificação de sigilo e trilhas de auditoria em nuvem
- **Lei do Governo Digital (Lei nº 14.129/2021):** princípios e instrumentos para serviços públicos digitais; reforça adoção de serviços em nuvem no Executivo

Decretos

- **Decreto nº 12.572/2025:** Institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação no âmbito da administração pública federal.
- **Decreto nº 10.046/2019:** Estabelece a governança de compartilhamento de dados entre órgãos federais e o Cadastro Base do Cidadão, exigindo base legal, interoperabilidade e rastreabilidade de acessos

Portarias

- **Portaria Nº 218/2020 (MF):** Institui a Política de Segurança da Info. do Min. Economia
- **Portaria Nº 5.827/2021 (MF):** Aprova a estrutura do Sistema de Gestão de Segurança da Informação do Ministério da Economia (SGSI)
- **Portaria Nº 5.950/2023 (SGD/MGI):** Define modelo obrigatório de contratação de software e serviços de computação em nuvem para órgãos e entidades do SISP do Poder Exec. Federal

Instruções normativas

- **Instrução Normativa Nº 1/2020 (GSI/PR):** Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal (GSI)
- **Instrução Normativa Nº 5/2021 (GSI/PR):** Requisitos mínimos de segurança da informação para utilização de nuvem pelo governo
- **Instrução Normativa nº 94/2022 (SGD/MF):** Processo de contratação de soluções de TIC pelos órgãos e entidades integrantes do SISP do Poder Executivo Federal
- **Instrução Normativa nº 8/2025 (GSI/PR):** Requisitos mínimos de segurança da informação para tratamento de informação classificada em computação em nuvem

Regulação de *Cloud* para setor privado (setoriais)

Sistema financeiro (Bacen)

- **CMN Res. 4.893/2021 + BCB Res. 85/2021:** política de segurança cibernética e requisitos de contratação de nuvem para instituições autorizadas a funcionar pelo Bacen

Seguros (SUSEP)

- **CNSP 416/2021:** Sistema de controles internos e estrutura de gestão de riscos e atividade de auditoria interna
- **SUSEP Circ. 638/2021:** requisitos de segurança cibernética a serem observadas pelas sociedades seguradoras, entidades abertas de previdência complementar (EAPCs), sociedades de capitalização e resseguradores locais

Saúde (ANS)

- **Lei 13.787/2018:** Digitalização e utilização de sistemas informatizados para guarda, armazenamento e manuseio do prontuário de paciente
- **ANS RN 443/2019:** adoção de práticas mínimas de governança corporativa, com ênfase em controles internos e gestão de riscos, para solvência das operadoras de plano de assist. à saúde

Telecomunicações (Anatel)

- **ANATEL Res. 740/2020:** Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações
- **ANATEL 780/2025:** Altera Regulamento de Avaliação de Conformidade e de Homologação de Produtos para Telecom

Energia elétrica (ANEEL)

- **ANEEL Res. 964/2021:** Política de segurança cibernética a ser adotada pelos agentes do setor de energia elétrica

Soberania de IA

A mesma lógica da nuvem vale para a IA: controlar onde ela roda, que dados trata e quem decide.

Onde roda

O QUE ESTÁ EM JOGO

IA operada fora do país segue as regras e as prioridades de quem a opera

O QUE A SOBERANIA PODE ORIENTAR

Nuvem de governo para o que é sensível e plano de saída do fornecedor
Acordos e contratos com fornecedor

Que dados trata

O QUE ESTÁ EM JOGO

Dado pessoal (LGPD) ou informação sigilosa (LAI e outras hipóteses de sigilo) inserido em IA sem base legal nem registro do uso

O QUE A SOBERANIA PODE ORIENTAR

Classificar o dado antes de usar a IA: dado pessoal e sigiloso só em ferramenta autorizada, com registro e auditoria

Quem decide

O QUE ESTÁ EM JOGO

Sistema que decide sobre direito do cidadão sem servidor que responda nem possibilidade de revisão

O QUE A SOBERANIA PODE ORIENTAR

Autonomia conforme risco e reversibilidade; ação que afeta direito tem humano responsável

A IA de ponta se concentra em EUA e China: em 2025, 50 e 30 modelos de destaque; nenhum outro país passou de 5.

O acesso à IA de ponta pode depender da política de outro Estado.

Fontes: IBM, Cost of a Data Breach Report 2026, p. 5; Stanford HAI, AI Index 2026; WEF, Empowering Defenders (2026), p. 27.

IA: novos riscos, velhas falhas

A IA amplia a capacidade de quem defende e de quem ataca, e as brechas estão no ambiente em volta dela.

INCIDENTES COM IA EM ORGANIZAÇÕES VIOLADAS

21%
tiveram incidente com IA (eram 13% um ano antes)

92%
das que tiveram incidente não tinham controle de acesso à IA

43%
dos incidentes envolveram IA não autorizada (eram 20%)

68%
não tinham governança de IA nem detecção de uso não autorizado (eram 63%)

IA AGÊNTICA: CASOS DE 2026

Hugging Face · julho

Agentes da OpenAI em teste comprometeram a infraestrutura da plataforma Hugging Face.

Governo da Austrália · junho

Um agente da OpenAI entrou no portal de estatísticas do Medicare. O governo da Austrália só foi avisado em setembro.

Para a IBM, os incidentes com IA vieram de falhas de governança, não do modelo: APIs e aplicações conectadas comprometidas e nuvem mal configurada. Na defesa, quem usa IA de forma extensiva identifica e contém violações em 215 dias, contra 280 sem IA.

O risco novo entra pelas falhas antigas: acesso, integrações e configuração.

Fontes: IBM, Cost of a Data Breach Report 2026, p. 3, 43, 47, 49 e 53; BBC News (set. 2026).

Como apoiamos a construção da Soberania Digital

O GSI/PR atua em cinco camadas para dar ao Estado capacidade de escolha:

Regras próprias

PNSI e PNCiber
Políticas nacionais

E-Ciber, E-SegInfo* e SISInfo*
- Estratégias
- *Sistema integrado**

Instruções Normativas
Orientação e regulação
- *Uso e desenvolvimento seguro de IA**

Plataformas soberanas

AtalaIA*
Governança, riscos e conformidade de SI com apoio de IA, em nuvem de governo

GuardIAo*
Sensores com IA para detectar e responder a ameaças nos órgãos

IA para o CTIR Gov
Modelo IA aberto, isolado, para apoio na triagem e classificação de incidentes

Resposta coordenada

CTIR Gov
Prevenção, tratamento e resposta a incidentes cibernéticos de governo

ReGIC
Rede federal que integra a gestão de incidentes dos órgãos

Pessoas e maturidade

Autodiagnóstico da PNSI
Mede a maturidade de segurança dos órgãos

Conscientização
Campanhas e capacitação de servidores

Cooperação

Informação classificada
Acordos de troca e proteção mútua com outras nações

Acordos e parcerias
Cooperação, parcerias e memorandos de entendimento

Foros internacionais
Representação do Brasil

** Em desenvolvimento*

IV CONGRESSO DE
DIREITO TRIBUTÁRIO
E ADUANEIRO
DA RECEITA FEDERAL

Tributação, Inteligência e Justiça Fiscal

Obrigado!

https://www.gov.br/gsi

APOIO

BID

MINISTÉRIO DA EDUCAÇÃO

REALIZAÇÃO

Receita Federal

MINISTÉRIO DA FAZENDA