# Soberania de Dados e LGPD em Contratações Públicas de Nuvem: Desafios e Limitações do Governo Federal

Ivan Garritano Barros Junior [1], Robson de Oliveira Albuquerque [1,2]

[1] *Programa de Pós-Graduação Profissional em Administração Pública (PGAP); Departamento de Administração (ADM), Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas (FACE), Campus Universitário Darcy Ribeiro; Universidade de Brasília (UnB), Asa Norte, 70910-900, Brasília/DF, Brasil*

[2] *Mestrado em Governança, Tecnologia e Inovação, Universidade Católica de Brasília – UCB Brasília, Brasil – Zipcode 71966-700*

*ivan.junior@aluno.unb.br; robson@redes.unb.br*

**Resumo**: A crescente digitalização dos serviços públicos, impulsionada pela Estratégia Federal de Governo Digital, tem acelerado a adoção da computação em nuvem nas instituições estatais. A significativa quantidade de informações pessoais e sensíveis processadas em infraestruturas tecnológicas de terceiros suscita relevantes preocupações relacionadas à proteção, privacidade e conformidade regulatória no tratamento destes dados. Este artigo analisa em que medida os atuais instrumentos de contratação e governança do Governo Federal, para serviços de computação em nuvem, garantem a soberania dos dados e a conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD). A pesquisa adota uma abordagem mista com aspectos qualitativos e quantitativos baseados na pesquisa documental e análise dirigida de contratos de tecnologia da informação (TI) do Governo Federal, complementados pela apreciação da iniciativa da "Nuvem de Governo" e um enfoque comparativo do contexto nacional com o panorama internacional sobre soberania de dados. Dentre os principais achados destacam-se a existência de lacunas contratuais sistêmicas, limitações da Nuvem de Governo e a imaturidade da base legal e estratégica nacional. As principais contribuições deste trabalho estão materializadas em proposições para o aprimoramento de um modelo mais robusto e soberano de adoção de nuvem pelo Estado.

***Palavras-chave:*** Soberania de Dados, LGPD, Responsabilidade Compartilhada, Nuvem, Conformidade, Setor Público.

## I. INTRODUÇÃO

A transformação digital do Estado brasileiro é um processo irreversível e estratégico, no qual a computação em nuvem emerge como alicerce tecnológico fundamental. Para o Governo Federal, a adoção de serviços de nuvem pode representar ganhos de eficiência, escalabilidade e inovação na prestação de serviços públicos. No entanto, essa crescente migração carrega consigo uma preocupação crítica sobre como conciliar a natureza global, multijurisdicional e frequentemente opaca dos provedores de serviços em nuvem com os imperativos nacionais de soberania, segurança e proteção dos dados dos cidadãos.

O cerne dessa preocupação reside na utilização de infraestruturas de nuvem de terceiros, para o tratamento de significativo volume de dados pessoais tutelados pela Administração Pública tais como informações de saúde, fiscais, previdenciárias e sociais. A Lei Geral de Proteção de Dados (LGPD) estabeleceu um marco ao conferir aos cidadãos direitos sobre seus dados e impor ao Poder Público, na condição de controlador, obrigações rigorosas de transparência, segurança e responsabilização. Paralelamente, a soberania de dados, como princípio fundador e a consequência estratégica da LGPD, transcende a mera localização geográfica dos servidores, demandando controle jurídico efetivo, independência operacional e resiliência contra a aplicação extraterritorial de leis estrangeiras.

Nesse cenário, o modelo de responsabilidade compartilhada da nuvem, que exige posturas de segurança por parte de clientes e provedores, coloca desafios práticos ao governo. Como exercer o controle determinante exigido pela LGPD sobre dados que residem em infraestruturas complexas e globais, se os mecanismos internos de acesso e processamento são, em grande medida, uma "caixa-preta"? A recente iniciativa da "Nuvem de Governo", fruto de um acordo entre empresas estatais de tecnologia e grandes provedores, busca responder parte dessa questão, promovendo a localização física de data centers em território nacional. Contudo, persiste a indagação fundamental: essa medida é suficiente para garantir a plena conformidade com a LGPD, especialmente quanto ao risco de transferências internacionais de dados e ao acesso por entidades estrangeiras?

Esta pesquisa parte da premissa de que os atuais instrumentos de contratação, governança e controle da nuvem pelo Governo Federal podem não estar adequadamente definidos para enfrentar o desafio de assegurar a soberania dos dados e cumprir integralmente a LGPD. A hipótese central é que existem lacunas significativas nos contratos e na governança interna que fragilizam a posição do Estado como controlador, tornando-o excessivamente dependente das garantias, por vezes genéricas, dos provedores. Para investigar esse problema, este artigo analisa criticamente a capacidade dos atuais mecanismos de contratação e governança de serviços de nuvem do Governo Federal em garantir, de forma efetiva e verificável, a soberania dos dados e a conformidade com a LGPD. A fim de analisar essa capacidade, busca-se: i) identificar e categorizar lacunas em contratos e editais públicos; ii) avaliar em que medida a iniciativa "Nuvem de Governo" mitiga os riscos à soberania e à proteção de dados e iii) avaliar comparativamente as práticas brasileiras em um panorama internacional.

A análise proposta é relevante pois, num enfoque pragmático, pode subsidiar órgãos e gestores públicos na melhoria das contratações. Sob o ponto de vista acadêmico, preenche uma lacuna na literatura nacional que conecta direito, administração pública e tecnologia de forma aplicada e, num prisma social, contribui para a proteção dos dados pessoais de milhões de cidadãos, fortalecendo a confiança nos serviços públicos digitais.

A estrutura do trabalho apresenta esta breve introdução seguida do referencial teórico, no qual são explorados os principais conceitos que fundamentam a pesquisa, em seguida, é detalhada a metodologia mista adotada, com aspectos qualitativos e quantitativos baseados na pesquisa documental e análise dirigida de contratos de TI do Governo Federal. Na seção de resultados, os achados das etapas anteriores são sintetizados, discutidos e as principais contribuições deste estudo incluem proposições para o aprimoramento dos processos de contratação de serviços em nuvem e recomendações para adoção de um modelo mais robusto e soberano em nuvem pelo Estado. Por fim, as conclusões fazem o fechamento do trabalho.

## II. REFERENCIAL TEÓRICO E REVISÃO DA LITERATURA

Para embasar a análise crítica proposta neste estudo, o referencial teórico percorre sete eixos fundamentais: i) o conceito de soberania de dados, essencial para delimitar o controle estatal sobre informações estratégicas em ambiente de nuvem; ii) a LGPD como parâmetro jurídico-normativo de conformidade e proteção de dados pessoais; iii) a computação em nuvem no setor público com as particularidades técnicas e contratuais da administração federal; iv) o modelo de responsabilidade compartilhada que permite identificar lacunas na alocação de deveres entre provedor e contratante; v) a governança de contratações em nuvem no governo, que revela a operacionalização dos mecanismos de controle e transparência; vi) a iniciativa da nuvem de governo como estratégia para garantir a soberania de dados e vii) o panorama internacional onde o contraste entre o Cloud Act (EUA) e a iniciativa GAIA-X (Europa) permite avaliar comparativamente o grau de autonomia e maturidade da estratégia brasileira. Esses tópicos, articulados, sustentam a verificação empírica dos desafios à soberania de dados e à LGPD nas aquisições públicas de nuvem.

### *A. Soberania de Dados*

A soberania de dados configura-se como um princípio essencial no cenário tecnológico atual, representando a capacidade de um Estado ou comunidade de estabelecer regras e exercer controle jurídico sobre as informações pessoais e coletivas geradas em seu território ou por seus cidadãos. Este conceito coloca em tensão a natureza global e fluida da internet com as fronteiras legais nacionais. Legislações como a Lei Geral de Proteção de Dados no Brasil, que busca equilibrar a livre circulação de informações com a garantia da privacidade e a segurança dos titulares, exemplificam ações destinadas a garantir a soberania de dados. Uma revisão sistemática da literatura sobre o tema deve, portanto, partir dessa definição fundamental e identificar as diferentes perspectivas sob as quais a soberania de dados pode ser avaliada.

Inicialmente, para reflexão crítica sobre este assunto, é importante compreender a ideia do “Capitalismo de Vigilância”, que descreve o modelo de negócios adotado por parte das Big Techs, no qual dados comportamentais de usuários se tornam o principal ativo econômico. Plataformas como Google, Meta, Amazon, Microsoft, Apple e TikTok coletam, de forma contínua, informações geradas por interações cotidianas (buscas, cliques, localização, tempo de uso, histórico de consumo e padrões de engajamento) para construir perfis detalhados que permitem prever e influenciar comportamentos em larga escala [1]. Esse modelo concentra poder informacional em corporações globais, que controlam infraestruturas digitais e serviços em nuvem frequentemente fora das jurisdições onde os dados são produzidos. Como resultado, decisões econômicas, sociais e informacionais passam a ser mediadas por interesses privados, o que impõe desafios à capacidade dos Estados de regular, proteger e governar dados estratégicos de seus cidadãos e instituições. Neste contexto, a soberania de dados surge como uma reação a essa extração predatória, permitindo que indivíduos e coletividades retomem o controle sobre suas informações [1].

Um fenômeno alinhado ao conceito do “Capitalismo de Vigilância” é o “Colonialismo de Dados”, que se trata da extração massiva de dados do Sul Global (abaixo da linha do Equador) por corporações do Norte (Big Techs),

reproduzindo relações coloniais de exploração [2]. A soberania de dados é ameaçada quando dados estratégicos (ex.: mercado de trabalho, saúde, educação, entre outros) são processados e armazenados fora do território nacional, sob jurisdição estrangeira [3]. Alguns exemplos citados na literatura são: i) o acordo realizado entre o Sistema Nacional de Emprego (SINE) e a Microsoft para uso de IA, com transferência de dados sensíveis do mercado de trabalho brasileiro e ii) o Ministério da Educação (MEC), que transferiu o processamento dos dados do Sistema de Seleção Unificada (SISU), com informações sensíveis de milhões de estudantes (notas, renda familiar, raça, deficiências), para a nuvem da Microsoft (Azure). O argumento foi o alto custo de manter um data center próprio. Esse caso é um exemplo paradigmático de como a lógica da economicidade imediata (reduzir custos) prevalece sobre considerações estratégicas de soberania e segurança nacional, colocando dados populacionais críticos sob jurisdição estrangeira [4]. Em geral, na era da computação em nuvem e das leis extraterritoriais, identificam-se as seguintes quatro dimensões críticas de controle que servem como pilares da soberania de dados [5] conforme apresentado na Tabela I.

*Tabela I – Pilares da Soberania de Dados*

| Pilar de Soberania | Descrição |
|---|---|
| Localização (Residência de Dados) | Capacidade de determinar onde os dados são armazenados e processados fisicamente para se submeter a leis locais específicas. |
| Controle Jurídico | Diz respeito à legislação que se aplica aos dados, independentemente de onde eles estão. Há um conflito crescente entre leis nacionais e a jurisdição territorial das Big Techs. |
| Controle Operacional | Capacidade de acessar, gerenciar e processar dados sem dependência de terceiros estrangeiros, garantindo a continuidade do serviço mesmo em crises geopolíticas. |
| Imunidade (Extraterritorialidade) | Refere-se à proteção contra acessos forçados por governos estrangeiros. |

*Fonte: Elaborado pelo autor*

Como argumentam Penteado, Pellegrini e Silveira [3], a soberania de dados nacional enfrenta desafios como a falta de regulação e políticas públicas. Estes autores consideram que o Brasil ainda carece de marcos regulatórios robustos para proteger os dados nacionais e a Lei Geral de Proteção de Dados é um passo ainda insuficiente diante do poder das plataformas. Neste contexto, defendem que o caminho para uma implementação efetiva da soberania de dados exige investimentos em infraestrutura pública de dados (data centers nacionais, redes públicas, hospedagem local) para reduzir a dependência de servidores estrangeiros, assim como o uso de software livre e hardware aberto para fortalecer a soberania tecnológica, permitir auditoria, adaptação local e fomentar inovação autônoma.

### *B. Lei Geral de Proteção de Dados (LGPD)*

A Lei Geral de Proteção de Dados (LGPD), promulgada em 2018 formalmente como Lei nº 13.709/2018, instituiu no Brasil um marco regulatório robusto para o tratamento de dados pessoais [6]. Inspirada em padrões globais, a LGPD estabelece um conjunto de direitos aos cidadãos e obrigações aos agentes que processam informações, redefinindo os parâmetros de licitude, segurança e transparência no ambiente digital e impondo novos requisitos às operações do governo federal [7]. No contexto da transformação digital do setor público, a conformidade com marcos regulatórios como a LGPD transcende a esfera jurídica para se consolidar como um desafio central de tecnologia da informação e governança [8]. A implementação efetiva da lei exige uma reavaliação profunda das arquiteturas de sistemas, dos protocolos de segurança e dos fluxos de dados. Dessa forma, a busca pela conformidade emerge como um vetor crítico para a modernização da infraestrutura estatal, demandando a convergência entre especialistas na lei, arquitetos de solução e gestores públicos.

A fim de melhor clarificar a compreensão a respeito da LGPD, é crucial abordar os pilares que traduzem o texto legal em implicações práticas. Na lei, dentre os conceitos cruciais destacam-se “dado pessoal” e “dado pessoal sensível”. A lei define dado pessoal como qualquer informação relacionada a uma pessoa natural identificada ou identificável (Art. 5º, I). Isso inclui desde nomes e CPFs até endereços de IP e dados de localização quando vinculados a um indivíduo. A categoria dos dados pessoais sensíveis (Art. 5º, II) recebe proteção reforçada por se referir a aspectos íntimos da personalidade, como origem racial, convicção religiosa, saúde e vida sexual. “Tratamento” é o conceito-operacional central, define-se como toda operação realizada com dados pessoais (Art. 5º, X), abrangendo coleta, armazenamento, uso, compartilhamento, até a eliminação. Na prática de TI, “tratamento” é sinônimo de processamento em bancos de dados, aplicações e servidores. A lei apresenta também um conjunto de atores com papéis e responsabilidades específicas (Art. 5º, VI-XII), a saber: Titular, Controlador, Operador, Encarregado e Autoridade Nacional de Proteção de Dados (ANPD).

Para além dos conceitos e atores, os princípios basilares desta legislação encontram-se no Art. 6º. Tais princípios

surgem como regras éticas e técnicas fundamentais que devem orientar todo e qualquer tratamento de dados pessoais. Eles são os alicerces que dão sentido prático à lei, exigindo, por exemplo, que o uso de dados tenha uma finalidade legítima, específica e informada ao titular (princípio da finalidade) e se limite estritamente ao mínimo necessário para alcançá-la (princípio da minimização). Outros princípios essenciais são a transparência, a segurança e a prestação de contas (accountability), que obriga o controlador a não apenas cumprir, mas a demonstrar o cumprimento da lei. Na prática da computação em nuvem, esses princípios demandam a adoção de arquiteturas de Privacy by Design e a revisão profunda de políticas de retenção e acesso a dados [9], o que por si só é um desafio significativo para usuários e administradores de sistemas.

No que se refere às garantias para os donos dos dados pessoais, a LGPD confere aos cidadãos (titulares) um conjunto de direitos instrumentais que os tornam agentes ativos no ciclo de vida de seus dados (Arts. 17 a 22). Esses direitos materializam o controle prometido pela lei, incluindo: direito de acesso e confirmação (saber se seus dados são tratados e acessá-los), direito de correção (retificar dados incompletos, inexatos ou desatualizados), direito à eliminação e à portabilidade (deletar dados ou solicitá-los em formato estruturado para transferi-los a outro serviço) e direito à explicação (receber informações claras sobre decisões tomadas com base em processamento automatizado).

Operacionalizar esses direitos é um desafio significativo para o governo, exigindo a criação de canais seguros, sistemas de rastreamento (*logging*) e interfaces que permitam atender a essas solicitações de forma ágil, auditável e em conformidade com prazos legais [10]. Para situações em que os dados pessoais sob custódia do governo precisam ser transferidos para fora do território nacional, a LGPD (Arts. 33 a 36) estabelece condições rígidas, assegurando que o nível de proteção não se perca no fluxo internacional. As principais vias legais para tal transferência são: i) para países ou organizações internacionais que proporcionem nível adequado de proteção, reconhecido pela ANPD, ii) por meio de garantias específicas, como cláusulas contratuais padrão aprovadas pela autoridade e iii) em hipóteses excepcionais previstas na lei, como para a execução de política pública.

Como apontam Oliveira et al. [10], longe de representar apenas um conjunto restritivo de regras, a LGPD configura-se como um poderoso indutor para a adoção de novas arquiteturas tecnológicas, padrões de segurança avançados e modelos de governança no setor público. Consequentemente, a conformidade deixa de ser um fim em si mesma para se tornar um catalisador de modernização, incentivando a adoção de serviços em nuvem com controles robustos e a estruturação de uma governança de dados clara. Desta forma, a LGPD assume um caráter instrumental primordial, ao erigir as bases normativas para a governança dos dados pessoais e estabelecer uma base que resguarda os cidadãos contra usos abusivos sendo, desta forma, o principal instrumento nacional para amparar as ações de soberania de dados.

### *C. Computação em Nuvem no Setor Público*

A adequada compreensão da nuvem e sua utilização no setor público exige uma compreensão inicial a respeito dos conceitos, características e modelos de serviço e implantação da nuvem. A computação em nuvem é definida como um modelo para permitir o acesso sob demanda a uma rede compartilhada de recursos computacionais (rede, servidores, armazenamento, aplicações e serviços) com o mínimo esforço de gerenciamento ou interação com o provedor de nuvem [11]. O Gartner dispõe que a computação em nuvem é um estilo de computação no qual capacidades habilitadas por TI, escaláveis e elásticas, são entregues como um serviço usando tecnologias da internet [12]. Outra definição, por parte da Agência Europeia para Cibersegurança, aponta que a computação em nuvem é um modelo de entrega de serviços de TI baseado em Internet, pelo qual os recursos são terceirizados, flexíveis, provisionados sob demanda, e com localização frequentemente indeterminada, pois o cliente pode não saber ou não controlar onde seus dados estão sendo processados ou armazenados fisicamente [13]. Em geral, as definições de computação em nuvem apontam cinco características essenciais: amplo acesso à rede, elasticidade (ou escalabilidade), serviço mensurável, autoatendimento sob demanda e compartilhamento de recursos [11, 14].

Conforme definições do National Institute of Standards and Technology (NIST), a oferta de serviços em nuvem se dá basicamente através de três modelos: Software as a Service (SaaS), Platform as a Service (PaaS) e Infrastructure as a Service (IaaS) [11]: i) no modelo SaaS o consumidor usa aplicativos do provedor executados em infraestrutura de nuvem, acessíveis via navegador web ou outras interfaces do cliente (smartphones, tablets), sem gerenciar a infraestrutura subjacente, exceto configurações limitadas de usuário, ii) no modelo PaaS, permite-se implantar aplicações criadas pelo consumidor usando linguagens, bibliotecas e ferramentas suportadas pelo provedor, que gerencia infraestrutura e middleware, mas o cliente controla as aplicações implantadas e iii) no modelo IaaS o consumidor provisiona recursos fundamentais como processamento, armazenamento e redes, implantando software próprio, com controle sobre sistemas operacionais e aplicações, mas sem gerenciar a infraestrutura física subjacente.

A literatura aponta quatro modelos de implantação de nuvem [14] para viabilizar a oferta dos serviços acima conceituados. Estes modelos de implantação são definidos pela natureza do público-alvo e pelo modelo de propriedade/gestão da infraestrutura: i) Nuvem Pública, para uso aberto pelo público em geral, onde os recursos (computação, armazenamento, rede) são de propriedade, gerenciados e operados por um provedor de serviços (terceiro) e compartilhados entre múltiplas organizações, ii) Nuvem Privada, para uso exclusivo por uma única organização. A

infraestrutura pode ser gerenciada pela própria organização, por um terceiro, ou combinação de ambos, e pode estar localizada nas instalações da organização (on-premises) ou externamente (hosted). O isolamento e o controle são máximos, iii) Nuvem Comunitária, que pode ser gerenciada pelas organizações da comunidade, por um terceiro, ou combinação de ambos. É um modelo de propriedade ou uso compartilhado por um grupo com necessidades alinhadas e iv) Nuvem Híbrida, composta por duas ou mais infraestruturas de nuvem distintas (pública, privada ou comunitária) que permanecem como entidades únicas, mas são ligadas por tecnologia padronizada ou proprietária que permite a portabilidade de dados e aplicações.

Na prática, os serviços em nuvem oferecem aos usuários uma abstração que permite acesso a recursos computacionais que, devido à facilidade com que podem ser escalados, parecem praticamente infinitos. Essa percepção de simplicidade e elasticidade possibilita que entes estatais provisionem capacidades sem se preocupar com a infraestrutura física, focando apenas em suas necessidades operacionais. Neste sentido, a crescente utilização da computação em nuvem no governo materializa o processo de migração para uma plataforma tecnológica sem altos investimentos iniciais, com maior flexibilidade para o dimensionamento dos serviços, e que proporciona redução de custos e maior segurança [15]. Contudo, a importância de usar a nuvem deve ser entendida não apenas como uma questão técnica ou uma medida para economizar gastos públicos. Para muitos governos, é uma estratégia que permite que as iniciativas de programas governamentais sejam implementadas mais rapidamente, de forma simples e com melhor qualidade para os cidadãos [15].

No governo brasileiro, a Estratégia Federal de Governo Digital (EFGD), é o documento que representa o planejamento estratégico relacionado à tecnologia da informação. Analisando o histórico de publicação das versões da EFGD durante os últimos 15 anos, identifica-se que a menção à tecnologia de nuvem é observada pela primeira vez no planejamento referente à 2014-2015, dispondo genericamente sobre a necessidade de “definição de um modelo de oferta de serviços em nuvem a ser implantado nos órgãos” [16, 17]. Somente no planejamento referente a 2020-2023 a computação em nuvem é abordada com metas mais objetivas tais como: “Migração de serviços de pelo menos 30 órgãos para a nuvem até 2022” [18]. Na estratégia para o ciclo de 2024-2027 se verifica a continuidade do fomento para utilização de plataformas de nuvem: “A Administração Pública Federal, com mais de 130 datacenters, enfrenta oportunidades de otimização e fragilidades associadas à disponibilidade e segurança. O compartilhamento e centralização desses ambientes, juntamente com a migração para a nuvem, são soluções em implementação” [19]. Neste sentido, a Secretaria do Governo Digital (SGD), do Ministério da Gestão e da Inovação em Serviços Públicos (MGI), desde 2020, estimula o uso de serviços de computação em nuvem por órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) do Poder Executivo Federal.

A utilização de nuvem é um elemento comum a todas as estratégias de transformação digital de países, sendo normalmente definida como a política de “nuvem em primeiro lugar” (*cloud first*), que são diretivas governamentais que determinam que as agências criem e executem seus sistemas de TI na nuvem pública [15]. No governo federal brasileiro, a política de “nuvem em primeiro lugar” está positivada na Instrução Normativa nº 94 de 2022 da SGD, que dispõe sobre o processo de contratação de soluções de TI no Poder Executivo e estabelece que: “Os órgãos e entidades que necessitem criar, ampliar ou renovar infraestrutura de centro de dados deverão fazê-lo por meio da contratação de serviços de computação em nuvem, salvo quando demonstrada a inviabilidade em estudo técnico preliminar da contratação” [20].

Na prática, este movimento de utilização de serviços e migração de infraestruturas para a nuvem parece não desacelerar, sobretudo pela orientação sobre o uso de nuvem para soluções de TI do Poder Executivo. Em geral, os gestores públicos federais têm ciência das oportunidades e responsabilidades associadas à computação em nuvem e, neste sentido, sobre suas percepções a respeito dos riscos, estudos indicaram que a maior parte dos gestores acredita nas vantagens dos aspectos de segurança e eficiência deste modelo (considerando disponibilidade, integridade e confidencialidade) se comparado aos riscos de gerenciar uma infraestrutura local. Porém, preocupações relevantes a respeito da contratação de serviços de nuvem, e a migração de dados e sistemas governamentais para estes serviços terceirizados também foram registradas [21].

É importante destacar que essa aparente facilidade para a utilização da nuvem mascara um paradoxo fundamental relacionado à complexidade monumental da arquitetura tecnológica subjacente, composta por data centers dispersos globalmente, milhares de servidores interconectados, redes de alta velocidade e orquestração automatizada de múltiplas camadas [22]. Esta complexidade, inerente a uma infraestrutura tecnológica heterogênea, expande sobremaneira os desafios para manutenção da segurança [23, 24]. Desta forma, as organizações públicas que se beneficiam desses serviços precisam estar continuamente atentas a uma miríade de ameaças emergentes que desafiam diretamente a privacidade, integridade e disponibilidade de seus ativos informacionais [25, 26, 27]. Evidenciando esta dualidade entre os benefícios e os riscos da nuvem no setor público, trabalhos anteriores identificaram os temas mais relevantes abordados nas publicações relacionadas ao assunto, conforme categorizado na Tabela II.

*Tabela II – Benefícios e riscos da computação em nuvem no setor público*

| Categoria | Tema de Pesquisa |
|---|---|
| Benefícios | Desempenho |
| | Redução de custos |
| | Escalabilidade |
| | Resiliência e continuidade de negócios |
| | Capacidade de manutenção |
| | Melhoramentos quanto à segurança |
| Riscos | Comprometimento da disponibilidade dos serviços em nuvem |
| | Defasagem entre recursos tecnológicos do setor público e do prestador de serviços em nuvem |
| | Falta de integridade dos dados e das informações |
| | Possibilidade do prestador de serviço de nuvem não ser auditável |
| | Vulnerabilidades quanto à segurança (acesso não autorizado, vazamento de dados e deficiências nos mecanismos de segurança referentes aos terceirizados) |
| | Questões legais (legislação transfronteiriça) |

*Fonte: Adaptado de* [28]

Para melhor evidenciar os riscos relevantes, uma lista das principais ameaças relacionadas à computação em nuvem foi elaborada a partir do "Top Threats to Cloud Computing 2024" [29], "OWASP Top 10 (2025)" [30] e relatórios de provedores de nuvem como Microsoft [31] e Google [32]. Para reforçar a importância da conformidade e demonstrar como falhas técnicas podem resultar em violações legais concretas, a Tabela III apresenta cada ameaça relacionada a princípios, artigos e obrigações da LGPD.

*Tabela III – Principais ameaças na nuvem e sua correlação com a LGPD*

| Ameaça/Vulnerabilidade | Descrição | LGPD |
|---|---|---|
| Vazamento de dados | Acesso, exposição ou exfiltração não autorizada de dados sensíveis armazenados em ambientes de nuvem. | ● Art. 6º, VI (Segurança)<br>● Art. 46 (Medidas de Segurança)<br>● Art. 48 (Notificação de Incidente) |
| Software malicioso (malware/APT) | Execução de código malicioso que explora vulnerabilidades em aplicações, serviços ou infraestruturas de nuvem. | ● Art. 6º, X (Prevenção)<br>● Art. 46 (Medidas de Segurança)<br>● Art. 47 (Governança) |
| Sequestro de contas | Comprometimento de credenciais que permite a um agente malicioso assumir identidades legítimas e realizar ações indevidas. | ● Art. 6º, VI (Segurança)<br>● Art. 46 (Medidas de Segurança) |
| Negação de serviço distribuída (DDoS) | Sobrecarga deliberada de recursos computacionais ou de rede visando à indisponibilidade dos serviços em nuvem. | ● Art. 6º, VI (Segurança - Disponibilidade)<br>● Art. 46 (Integridade e Acesso) |
| Falhas de controle de acesso e IAM | Autorização inadequada ou excessiva a recursos de nuvem decorrente de políticas de identidade e acesso mal configuradas. | ● Art. 6º, III (Minimização)<br>● Art. 6º, VI (Segurança)<br>● Art. 46 e 47 (Governança) |
| Vulnerabilidades de virtualização | Falhas nos mecanismos de isolamento entre máquinas virtuais ou camadas de abstração da infraestrutura. | ● Art. 46 (Medidas Técnicas Adequadas) |
| Perda de governança sobre dados | Redução do controle do cliente sobre dados, políticas de segurança e processos operacionais no ambiente de nuvem. | ● Art. 6º, II (Finalidade)<br>● Art. 47 (Governança - Accountability)<br>● Art. 7º e 11 (Bases Legais) |
| Erro humano e falta de conscientização | Incidentes de segurança causados por configurações incorretas, práticas inseguras ou desconhecimento dos usuários. | ● Art. 50 (Treinamento)<br>● Art. 47 (Cultura de Governança)<br>● Art. 42, §1º (Responsabilidade) |
| Criptografia inadequada ou mal gerida | Uso de mecanismos criptográficos fracos, obsoletos ou com gestão ineficiente de chaves de segurança. | ● Art. 6º, VI (Segurança)<br>● Art. 46 (Medidas Técnicas) |
| Interfaces e APIs inseguras | Vulnerabilidades em APIs, endpoints e mecanismos de integração. | ● Art. 46 (Proteção dos Canais)<br>● Art. 6º, VI (Segurança) |
| Recursos de terceiros inseguros | Riscos associados à cadeia de suprimentos, provedores e dependências externas. | ● Art. 26 (Responsabilidade Solidária) |

| | | |
|---|---|---|
| | | • Art. 37 (Contratos com Operadores)<br>• Art. 33 (Transferência Internacional) |
| Visibilidade e observabilidade limitadas | Dificuldades de monitoramento, auditoria, logging e resposta a incidentes. | • Art. 47 (Accountability / Governança)<br>• Art. 48 (Notificação)<br>• Art. 18 (Direitos do Titular) |

*Fonte: Elaborado pelo autor*

Para mitigar vulnerabilidades e prover conformidade com o arcabouço regulatório nacional, grandes provedores de nuvem realizam esforços para demonstrar alinhamento com a LGPD e subsidiar clientes com boas práticas e recursos para atender as exigências da lei. Tais provedores declaram-se "Cloud Compliant" e documentam como podem operar dentro dos rigores legais de dados no Brasil. Enquadram-se como exemplo destas iniciativas: "Brazil General Data Protection Law Workbook" [33], "Navigating LGPD Compliance on AWS" [34], "Google Cloud & Lei Geral de Proteção de Dados (LGPD)" [35] e a "HUAWEI CLOUD Compliance Instruction with Brazil LGPD" [36].

O investimento do governo é uma boa métrica para indicar como o paradigma de computação em nuvem tem alcançado importância e se tornado tendência na administração federal. Um recorte detalhado para o período mais recente (jan/2023 a jun/2025) indica que os gastos com soluções de computação em nuvem totalizaram R$ 9 bilhões representando cerca de 53% do total investido, ultrapassando os valores investidos em licenças de software (R$ 5,97 bilhões) e softwares/serviços de segurança digital (R$ 1,91 bilhão). Também se verifica a concentração dos contratos em poucas empresas globais, com destaque para Microsoft, Oracle, Google e Red Hat, representado a escolha por um ecossistema de fornecedores relativamente restrito [37]. Assim, segundo Ginglass [38], além dos riscos inerentes ao tratamento de dados em ambientes de nuvem, é necessário considerar os desafios à soberania tecnológica decorrentes da dependência de insumos críticos estrangeiros como sistemas operacionais, hardware, sistemas gerenciadores de banco de dados (SGBDs) e outros softwares essenciais. Estes componentes, desenvolvidos e mantidos por corporações ou Estados estrangeiros, podem ser objeto de manipulação para a inserção deliberada de vulnerabilidades ("backdoors") que atendam a interesses geopolíticos ou comerciais externos, risco que persiste mesmo quando a infraestrutura de processamento está fisicamente localizada em solo nacional .

De toda forma é importante destacar que a adoção de nuvem no governo é um fenômeno complexo e multidimensional, pois a simples disponibilidade da tecnologia não garante seu sucesso. Este sucesso depende da combinação e maturidade dos aspectos organizacionais (com estratégia clara, equipe dedicada e processos definidos), institucionais (com regulação específica, apoio político e governança) e contextuais (com mercado de TI desenvolvido e ecossistema de fornecedores) [39].

*D. Responsabilidade Compartilhada no Serviço Público*

O modelo de responsabilidade compartilhada forma a espinha dorsal da segurança em ambientes de nuvem, definindo as obrigações de segurança do provedor de serviços e do cliente. Em geral, o provedor gerencia a segurança da infraestrutura de nuvem, incluindo sua segurança física e de rede, e os clientes são responsáveis por proteger seus próprios dados e aplicativos, além de gerenciar a identidade e os controles de acesso. O modelo varia ligeiramente dependendo do tipo de serviço em nuvem (o cliente detém a responsabilidade pela segurança, ainda que limitado a certas áreas operacionais), mas o princípio fundamental permanece o mesmo: ambas as partes compartilham a responsabilidade de manter um ambiente de nuvem seguro [40]. É essencial que os clientes de serviços em nuvem estejam familiarizados e atualizados sobre como eles e seus provedores de serviços compartilham a responsabilidade pela segurança de sua presença na nuvem. Isso implica desenvolver uma compreensão precisa de quem é responsável por quais funções de segurança (por exemplo, aplicação de patches, verificação de malware, análise de logs, provisionamento de usuários, etc.) [41].

Para auxiliar a melhor compreensão das nuances a respeito do modelo de responsabilidade compartilhada, a Figura 1 apresenta os modelos de responsabilidade utilizados pelas empresas Microsoft e Google. A apreciação destes modelos permite observar uma escalada crescente da responsabilidade exclusiva do cliente (considerando a sequência: SaaS, Paas e IaaS). Nestes arranjos, apesar de algumas atividades serem de responsabilidade exclusiva do cliente, isto não significa que os provedores de serviço em nuvem sejam meros espectadores em relação a isso, constata-se que os provedores oferecem apoio e orientação aos clientes para implementar os controles de segurança adequados. Contudo os clientes são, em última instância, responsáveis pela configuração segura dos serviços que consomem [41]. É importante ter ciência de que estes apoios técnicos não transferem a responsabilidade pois, apesar da oferta de suporte e ferramentas, a decisão e a implementação de boas práticas para configurar e proteger identidades e dados é dever do cliente. De forma semelhante, considerando a responsabilidade compartilhada sob o prisma da conformidade, os provedores "cloud compliant" assessoram seus clientes sobre recursos nativos das plataformas para atender às

exigências da LGPD, todavia a decisão sobre a efetividade de tais recursos e sua implementação cabe unicamente ao cliente da nuvem (neste contexto, o governo como controlador de dados).

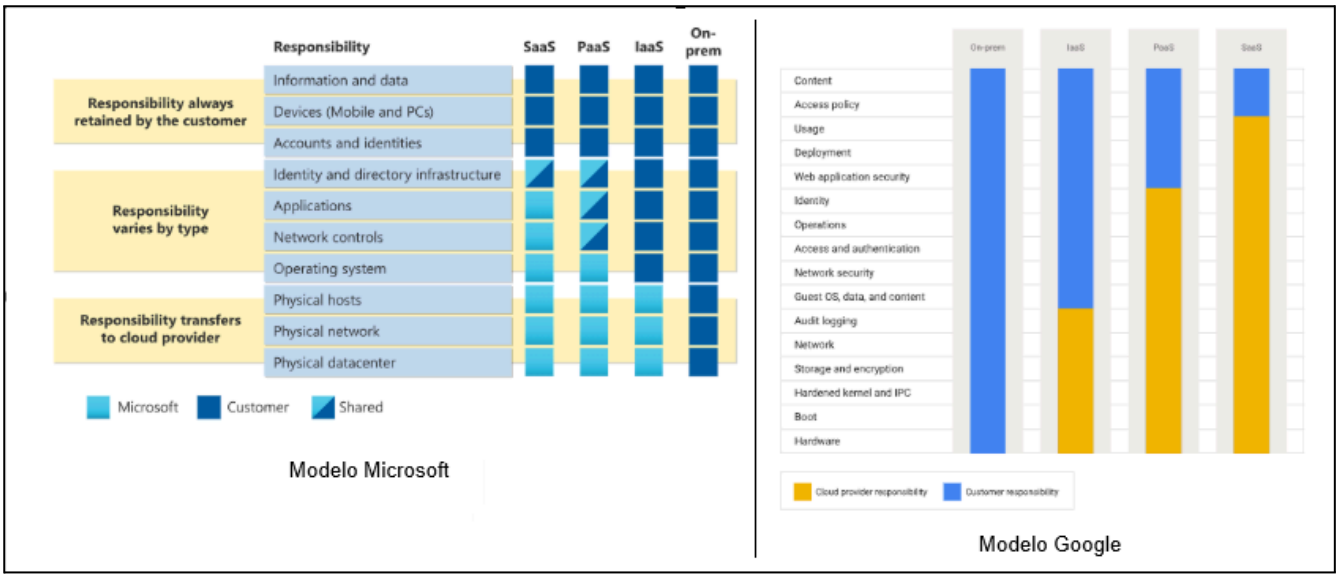


*Figura 1 – Modelos de Responsabilidade Compartilhada*
*Fonte: [42, 43]*

Com a consolidação da utilização dos serviços em nuvem, se tem observado o aumento da consciência por parte dos clientes a respeito de sua responsabilidade no processo. Estudos indicam que clientes têm desejado mais transparência sobre os programas de segurança operacional (SecOps) de seus provedores de nuvem, pois, para compreender e operacionalizar suas próprias obrigações de segurança, desejam entender melhor como estes provedores protegem a infraestrutura subjacente [41]. Geralmente essa confusão sobre os limites de responsabilidade pode levar a configurações insuficientes e gerar incidentes de segurança, e é justamente aí que reside um dos principais desafios no modelo de responsabilidade compartilhada, a falta de capacidade interna das equipes.

A Cloud Security Alliance (CSA) alerta que a má configuração continua sendo a principal ameaça à segurança na nuvem, um risco diretamente ligado à falta de conhecimento especializado [29]. Quando as equipes operacionais não compreendem novos paradigmas, como por exemplo, infraestrutura como código (IaC), que permite automatizar a aplicação de políticas de segurança, elas inadvertidamente criam brechas que neutralizam os controles de segurança oferecidos pelos provedores. Para tornar o cenário ainda mais complexo, os provedores de nuvem adicionam constantemente novos serviços funcionais às suas plataformas, com ferramentas exclusivas para gerenciamento da configuração e segurança. Os clientes de nuvem precisam estar atentos ao que está disponível e em uso em sua infraestrutura de nuvem para garantir que a postura de segurança cibernética da organização não seja afetada negativamente [44].

Em um ambiente de governo, é possível estender a análise da responsabilidade compartilhada para além da relação entre provedor e cliente apenas, e ponderá-la como uma responsabilidade compartilhada horizontal e colaborativa entre múltiplos atores para a segurança cibernética. Essencialmente em estruturas de governo, pode ser útil estabelecer redes de cooperação onde organizações, setores e entes estatais possam compartilhar informações, inteligência de ameaças e recursos. Contudo, a responsabilidade compartilhada nesta abordagem colaborativa enfrenta desafios e barreiras para sua implementação tais como [45]: i) compartilhar informações melhora a segurança coletiva, mas também pode expor vulnerabilidades e aumentar o risco, ii) como estabelecer confiança entre colaboradores sem comprometer a privacidade ou segurança operacional? e iii) responsabilidades legais (como LGPD) podem conflitar com o desejo de compartilhamento pleno.

Em instrumentos contratuais, considerando a temática de responsabilidade compartilhada, é importante mencionar sobre o “Cloud Data Processing Addendum (CDPA)”. O CDPA é uma espécie de termo de serviço que oferece garantias contratuais de proteção de dados e formaliza, na computação em nuvem, o regime de responsabilidade compartilhada entre cliente (controlador) e provedor (operador). Consolidado, entre 2015 e 2018, como padrão de mercado pelos grandes provedores, sua origem está diretamente ligada à iminência do GDPR (legislação europeia para a proteção de dados) e à necessidade de atender, de forma escalável, às exigências contratuais impostas pelas leis de proteção de dados. O CDPA estabelece as condições técnicas e jurídicas para o processamento de dados pessoais, assegurando conformidade com leis como a LGPD e a própria GDPR. Seu conteúdo abrange medidas de segurança, regras para

transferência internacional de dados (incluindo cláusulas contratuais padrão), notificação de incidentes e controle sobre sub-operadores. Trata-se do instrumento que confere previsibilidade jurídica e segurança à relação contratual ao traduzir obrigações legais em compromissos formalmente exigíveis. Exemplos representativos desse modelo são o AWS Data Processing Addendum [46] e o Aditivo sobre Tratamento de Dados do Cloud (clientes) do Google [47]. O CDPA constitui, portanto, uma resposta da indústria de tecnologia à necessidade de escalabilidade e previsibilidade jurídica no tratamento de dados pessoais em ambientes de nuvem. Ao estabelecer cláusulas padronizadas, incluindo cláusulas contratuais padrão (Standard Contractual Clauses ou SCCs) para transferências internacionais, prazos de notificação de incidentes e controles sobre sub operadores, o CDPA funciona como um instrumento de *due diligence* (uma investigação profunda e minuciosa realizada antes de contratos importantes) pré-contratual que reduz a assimetria de informações entre provedor e cliente.

Todavia, o modelo tradicional de responsabilidade compartilhada tem sido alvo de críticas, pois apesar de ser teoricamente sólido, falha na prática devido à complexidade operacional, falta de expertise dos clientes e baixa visibilidade, sobretudo em ambientes multi-nuvem que exigem aplicar políticas uniformes e gerenciar ferramentas diversas entre provedores distintos. Assim, considerando o tradicional modelo de responsabilidade compartilhada e o aumento de automação nas pipelines de desenvolvimento seguro (DevSecOps), bons modelos de responsabilidade passam a vincular segurança ao ciclo de desenvolvimento e não apenas à infraestrutura tradicional. Ferramentas de automação, especialmente para detecção de configuração insegura, tornam-se essenciais para reduzir falhas associadas a atribuições de responsabilidade ineficazes. Ferramentas de infraestrutura como código, com "security scanning" nativo e políticas de segurança automatizadas (Policy as Code) permitirão que organizações cumpram sua parte no modelo de forma proativa [48]. Outras tendências indicam o "Modelo de Destino Compartilhado" (Shared Fate), como uma evolução paradigmática, saindo da delegação para a co-propriedade, onde o provedor assume um papel mais ativo e colaborativo, ajudando proativamente o cliente a proteger seu ambiente [42, 49]. É um passo além da mera divisão de tarefas. Neste modelo há um alinhamento de incentivos entre provedores e clientes por meio de monitoramento contínuo de segurança, detecção colaborativa de ameaças e validação de aplicações.

Em todo caso, a transição para a nuvem deve ser acompanhada por uma transformação paralela e igualmente crítica que envolve o investimento massivo no desenvolvimento de capacitação interna. O modelo de responsabilidade compartilhada não é uma divisão binária, mas um contrato de colaboração onde o cliente deve manter sua parte do acordo. Organizações que subestimam essa necessidade transformam um modelo projetado para aumentar a agilidade e a segurança em um ponto cego operacional crítico, onde a sofisticação do provedor pode ser anulada pela própria inabilidade interna.

### *E. Governança de contratações de serviços em nuvem*

Entende-se como governança o conjunto de princípios, mecanismos e regras (liderança, estratégia e controle) usados para administrar, dirigir e monitorar organizações ou políticas públicas. Este estudo investiga os principais marcos (leis, portarias, instruções normativas etc.) mais diretamente relacionados ao uso de nuvem e à governança de contratações desses serviços, sem abordar detalhes normativos ou as minúcias procedimentais desses instrumentos. O propósito consiste em realizar uma revisão crítica, com foco na análise de seus fundamentos e evolução normativa, para delinear um panorama geral sobre como tais instrumentos assessoram os gestores públicos na ontratação de serviços de computação em nuvem. A Tabela IV apresenta estes marcos de forma cronológica.

*Tabela IV – Marcos relevantes para a governança de contratações de nuvem*

| Ano | Marco | Descrição |
|---|---|---|
| 2015 | Acórdão TCU nº 1.739/2015 | Auditoria sobre riscos em contratações de serviços sob o modelo de computação em nuvem. |
| 2020 | Instrução Normativa GSI/PR nº 1/ 2020 | Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal. |
| 2021 | Instrução Normativa GSI/PR nº 5/2021 | Requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal. |
| 2023 | Portaria SGD/MGI nº 5.950/2023 | Modelo de contratação de software e de serviços de computação em nuvem. |
| 2025 | Instrução Normativa GSI/PR nº 8/2025 | Dispõe sobre os requisitos mínimos de segurança da informação para tratamento de informação classificada em computação em nuvem. |

*Fonte: Elaborado pelo autor*

Inicialmente, destaca-se um relatório de auditoria elaborado em 2015 pelo Tribunal de Contas da União (TCU). Trata-se do Acórdão nº 1.739/2015, destinado à identificação de riscos relevantes em contratações de serviços sob o modelo de computação em nuvem no governo [50]. Muitos dos riscos identificados nesta auditoria se relacionam diretamente à segurança da informação (SI) e já foram mencionados neste estudo: indisponibilidade do serviço, confidencialidade e integridade de dados, auditabilidade, falhas em APIs e atualizações e correções de segurança. Porém, o relatório aponta para outras categorias de problemas que merecem destaque como os riscos relacionados à contratação e gestão contratual de serviços em nuvem. A Tabela V indica estes achados de auditoria.

*Tabela V – Riscos na contratação de serviços em nuvem conforme Acórdão TCU nº 1.739/2015*

| Categoria de Risco | Risco |
|---|---|
| Gestão Contratual | Níveis de serviço estabelecidos em contrato podem não ser cumpridos. |
| | Vulnerabilidades e problemas de segurança detectados no provedor demoram para ser corrigidos ou não são corrigidos. |
| | Falhas no monitoramento e gestão contratuais. |
| | Estouro de orçamento para o contrato devido à falta de controle sobre o uso dos recursos de computação em nuvem e estimativas imprecisas de custo. |
| Dependência frente ao provedor | Dependência do cliente com relação ao provedor (vendor lock-in). |
| | Dificuldades do cliente em migrar dados de um provedor para outro ou internalizá-los novamente, por problemas de interoperabilidade ou de portabilidade. |
| | Falta de previsão dos custos de saída do provedor. |
| | Indisponibilidade do fornecedor (ruptura contratual, falência, sequestro de dados). |
| Falhas contratuais | Conflitos sobre a propriedade dos dados armazenados na nuvem. |
| | Falta de delimitação legal regendo as relações contratuais, dado que os serviços de nuvem podem ser prestados globalmente. |
| | Não exclusão de dados armazenados na nuvem ao término de um contrato. |

*Fonte: Elaborado pelo autor*

Com base nos achados desta auditoria, evidencia-se que a gestão contratual de serviços em nuvem no âmbito público demanda uma abordagem multidisciplinar por parte do gestor, transcendendo a mera supervisão administrativa. A complexidade dos riscos identificados, que englobam desde a garantia de cumprimento de níveis de serviço (SLA) e a correção ágil de vulnerabilidades técnicas até o controle financeiro rigoroso para evitar estouros orçamentários, exige um domínio integrado de conhecimentos jurídicos (para estruturar cláusulas de propriedade de dados, portabilidade e resolução de conflitos), tecnológicos (para monitorar a segurança e a interoperabilidade) e de governança financeira (para gerar métricas de bilhetagem e elaborar estimativas de custos precisas, inclusive de saída). Portanto, o gestor público atuante nesse contexto deve conjugar essas diferentes dimensões, transformando-se em um articulador crítico que não apenas compreende os aspectos legais, técnicos e econômicos de forma isolada, mas principalmente os integra para mitigar riscos, assegurar a continuidade dos serviços e promover contratos eficientes, eficazes e economicamente sustentáveis.

Para a governança contratual em ambientes de nuvem, onde as decisões sobre aspectos tecnológicos tornam-se ainda mais críticas, faz-se necessário dotar os órgãos públicos com a capacidade operacional adequada para deliberar e tratar questões afetas à segurança da informação. Assim, convém destacar a Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020 [51], que define a estrutura de gestão da segurança da informação nos órgãos da administração pública federal. Este dispositivo se relaciona de forma estrutural e crítica com a governança de contratações de nuvem ao estabelecer o arcabouço organizacional mínimo para a gestão da segurança da informação. Ao exigir a designação de um Gestor de Segurança da Informação, um Comitê de Segurança da Informação e uma Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR), o dispositivo cria os atores e os fóruns especializados responsáveis por assessorar e embasar as decisões dos gestores contratantes. Portanto, a IN GSI/PR Nº 1/2020 não trata diretamente dos contratos de nuvem, mas fornece a estrutura de governança de segurança necessária ao suporte técnico e decisório. Ela objetiva assegurar que, dentro do órgão público, existam competências especializadas para orientar o gestor contratante desde a análise preliminar de riscos até a resposta a incidentes, integrando a segurança da informação como um pilar fundamental do ciclo de vida da contratação de serviços em nuvem.

Após a instrução normativa (IN) nº 1 de 2020, o GSI publicou, no ano seguinte, a Instrução Normativa GSI/PR nº 5/2021, que dispôs sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos da administração pública federal [52]. Este novo normativo endereçou a preocupação com a segurança da informação na computação em nuvem, atribuiu responsabilidades para os atores outrora estabelecidos e

indicou elementos obrigatórios para os instrumentos contratuais celebrados pelo governo federal. A análise deste documento permite constatar uma imposição à administração pública federal de um processo criterioso de *due diligence*, pois transfere ao órgão contratante responsabilidades que vão muito além da simples aquiescência às cláusulas do provedor. A norma exige que o órgão realize, previamente à contratação, o gerenciamento de riscos e a análise de impacto de dados pessoais (art. 11, II), além de avaliar criticamente a capacidade técnica do provedor em aspectos como práticas de fortalecimento de virtualização, testes de penetração, programa de correção de vulnerabilidades e conformidade com padrões internacionais de auditoria (art. 20, II, IV e XIV). Dentre as exigências preconizadas por esta IN de 2021 vislumbram-se conceitos já apresentados como "Soberania de Dados" (art 18, I e III) e "Responsabilidade Compartilhada" (art 16, II e III). Todas essas exigências convertem a *due diligence* em um dever de investigação aprofundada, no qual o contratante deve verificar evidências documentais, como os relatórios SOC 2 Tipo I e II, e não apenas declarações formais de boa-fé. Ademais, a obrigação de incluir determinados dispositivos no contrato exige que a *due diligence* abranja não somente a fase pré-contratual, mas também a capacidade operacional e a idoneidade do provedor para cumprir tais obrigações ao longo de toda a execução contratual.

Uma vez estabelecida a estrutura de gestão de segurança da informação nos órgãos (IN GSI 01/2020) e os requisitos de segurança da informação para a computação em nuvem (IN GSI 05/2021), em 2023, a Secretaria de Governo Digital estabeleceu o modelo de contratação de software e de serviços de computação em nuvem, através da portaria SGD/MGI nº 5.950, de 26 de outubro de 2023 [53]. Sobre este modelo de contratação é interessante destacar que, logo na introdução do seu Anexo I, são referenciados explicitamente quatro acórdãos do TCU que são a chave para entender a essência desta portaria. Estes acórdãos são unânimes em criticar fragilidades no planejamento da contratação que levam a superfaturamento, métricas de remuneração não verificáveis e falta de parâmetros para aferir a economicidade e a vantajosidade destes ajustes. Esta portaria é, portanto, uma resposta direta do órgão central (SGD) a essas determinações e recomendações do TCU. O objetivo é fornecer um modelo que blinde as contratações contra esses problemas crônicos de gestão de custos. A portaria SGD nº 5.950/2023 não inova ao tratar de segurança, ela apenas reforça a obrigação de cumprir a norma de segurança já positivada (IN GSI 05/2021). A grande inovação desta portaria é criar um modelo de contratação que discipline a relação custo-benefício, algo que era um vácuo normativo e a principal fonte de preocupação para a administração pública em contratações de nuvem. A segurança da informação é um requisito obrigatório e crítico, mas a governança dos custos e a definição de métricas justas e auditáveis emergem como o desafio operacional e jurídico que a Portaria SGD/MGI nº 5.950/2023 busca equacionar. É importante mencionar que havia nesta portaria vedação explícita ao uso de nuvem para o tratamento de informação classificada (reservada, secreta e ultrassecreta) nos termos da Lei de Acesso à Informação, conforme os seguintes termos: "informação classificada em grau de sigilo e documento preparatório que possa originar informação classificada não poderão ser tratados em ambiente de computação em nuvem".

Todavia, em 2025, o GSI publicou a Instrução Normativa nº 8/2025, que dispõe sobre os requisitos mínimos de segurança da informação para tratamento de informação classificada em computação em nuvem [54], o que acabou por revogar a vedação presente na portaria de 2023 da Secretaria de Governo Digital. O espírito desta nova instrução normativa do GSI é o de modernizar e flexibilizar a segurança nacional, permitindo, pela primeira vez, que informações classificadas sejam tratadas em nuvem, mas sob a necessidade de um rígido regime de controle estatal. A norma representa uma evolução da postura defensiva e proibitiva do passado para uma postura de permissão condicionada e regulada, reconhecendo os benefícios tecnológicos da nuvem e preocupando-se com a soberania e o alto nível de proteção. Ela disciplina e propõe, na prática, um "ambiente de nuvem soberano" exclusivo para o Estado brasileiro.

Para atingir esse objetivo, a Instrução Normativa nº 8/2025 estabelece um conjunto de requisitos rigorosos. Ela restringe os modelos de nuvem, somente sendo permitidas nuvens privadas ou comunitárias geridas por órgãos de registro ou postos de controle habilitados (art. 2º), eliminando qualquer possibilidade de uso de nuvens públicas para esses dados. Impõe-se uma série de garantias de soberania e segurança, como a localização compulsória de data centers em território nacional (art. 5º), a vedação de backups no exterior (art. 5º), a exigência de credenciamento de segurança de todo pessoal envolvido (arts. 7º, VIII, e 9º, III) e a obrigatoriedade de contrato sigiloso (art. 9º, I). A norma também eleva o padrão técnico ao exigir certificações específicas (ISO 27001, 27017, 27018, 27701 e 22237) e controles como criptografia com algoritmos de Estado e gerenciamento exclusivo de chaves pelo órgão público (art. 3º). É importante registrar que a vedação permanece para o mais alto grau de sigilo, ou seja, informações ultrassecretas continuam proibidas de serem tratadas em nuvem (art. 6º).

Considerando-se o foco deste trabalho, todas estas legislações utilizadas como referência para governança das contratações foram avaliadas com objetivo de se identificar dispositivos que orientem pela inclusão de cláusulas contratuais relacionadas à soberania de dados e conformidade com a LGPD. A análise permitiu identificar 28 dispositivos que foram consolidados e originaram a "Matriz de Requisitos Contratuais" (MRC), um instrumento central de análise deste estudo apresentado na seção III deste artigo.

*F. Nuvem de Governo*

A Nuvem de Governo, coordenada pelo Ministério da Gestão e da Inovação em Serviços Públicos (MGI) em parceria com o Serpro e a Dataprev, surge como uma iniciativa para a chamada "soberania digital" do Estado brasileiro. A proposta central é proteger os dados sensíveis da administração pública federal como, por exemplo, informações fiscais, previdenciárias, políticas de saúde e educação, para garantir que seu armazenamento e processamento ocorram sob total jurisdição da legislação brasileira e em território nacional [55]. Isto é muito conveniente, pois para a adoção de serviços de nuvem por parte do governo federal, a transferência internacional de dados é sempre uma questão crítica. Contratos com provedores globais devem prever explicitamente a base legal para a transferência (como cláusulas contratuais padrão) e as salvaguardas técnicas (como criptografia com chaves sob posse do governo) para garantir a soberania e a continuidade da proteção jurídica brasileira, sob pena de a operação configurar uma violação grave à lei [39]. Neste sentido, o uso da nuvem de governo, em tese, reduz as possibilidades de transferências internacionais de dados indevidas.

O modelo propõe duas camadas de soberania: a soberania dos dados, com residência estritamente nacional, e a soberania operacional, onde a gestão é executada exclusivamente por técnicos de empresas públicas em data centers próprios. Desta forma é possível proteger informações críticas contra ameaças cibernéticas e ingerências externas e, ao mesmo tempo, modernizar a infraestrutura de TI do Estado, com uso de tecnologias de ponta, como inteligência artificial, para melhorar os serviços públicos [56].

Na prática, a operacionalização da nuvem de governo revela um modelo híbrido interessante. Ao invés de de construir um ecossistema de tecnologia 100% nacional do zero, o governo federal optou por posicionar o Serpro e a Dataprev como "*cloud brokers*" estatais, com a condição de que as tecnologias das Big Techs sejam trazidas para dentro dos “muros” do Estado. O governo contrata a instalação de nuvens privadas das gigantes de tecnologia dentro dos datacenters do Serpro (em Brasília, São Paulo e Rio de Janeiro) e da Dataprev. O Serpro, por exemplo, assinou um contrato de 10 anos com o Google para provisionar uma unidade do Google Distributed Cloud em suas instalações, além de utilizar tecnologias da AWS e da Oracle para bancos de dados. A Dataprev, por sua vez, firmou acordos com Oracle, Huawei e AWS [57]. Neste arranjo, o governo adquire o software, as plataformas e as ferramentas de gestão das Big Techs, mas a operação, o controle de acesso e a governança dos dados são realizados por funcionários públicos do Serpro e da Dataprev. Assim, ao trazer a infraestrutura para data centers próprios e manter a operação sob gestão de estatais, o governo mitiga o risco de acesso não autorizado por jurisdições estrangeiras (como o Cloud Act norte-americano) e visando garantir que dados sigilosos estejam protegidos pela lei brasileira.

A concentração de dados críticos em nuvem privada governamental pressupõe ambientes controlados e com altos padrões de segurança (física e cibernética), através da utilização de uma infraestrutura mais robusta e com planos de recuperação de desastres, algo que, segundo pesquisa citada pelo Serpro, é deficitário em 69% dos datacenters de órgãos públicos [56]. Outra vantagem é permitir que o Estado utilize o que há de mais moderno em termos de computação em nuvem, como análise de dados e inteligência artificial, sem abrir mão do controle sobre seus ativos mais valiosos: as informações dos cidadãos. O Serpro considera o projeto como um "marco na soberania digital do país" e demonstra a intenção de "treinar modelos de IA que respeitem as especificidades culturais, linguísticas e legais do Brasil" [57].

Quanto à soberania de dados, o modelo da nuvem de governo opera exclusivamente em território nacional e os dados são protegidos por criptografia com gestão exclusiva das chaves em infraestrutura totalmente isolada, sem qualquer tipo de orquestração externa ou conexão com nuvens públicas estrangeiras. Destaca-se ainda que nenhuma informação da nuvem de governo é replicada ou enviada sem autorização, e que toda a operação é feita exclusivamente por técnicos das estatais. Não obstante o uso de tecnologias estrangeiras, as empresas públicas afirmam dominar toda a gestão e manutenção dessas plataformas, e que isto representa na prática soberania operacional e tecnológica [56].

Porém, há outros pontos de vista que sustentam que o atual modelo de operacionalização da nuvem soberana, embora mantenha os dados em território nacional, pode estar criando uma dependência tecnológica de novo tipo. O risco é que as empresas públicas se transformem em "balcões de negócios" das Big Techs, operacionalizando uma soberania apenas formal (pela localização dos dados), mas comprometendo a soberania em sua dimensão material, isto é, a capacidade real do Estado de controlar efetivamente a tecnologia, desenvolver capacidades próprias e evitar a subordinação de seus interesses estratégicos às lógicas comerciais das corporações estrangeiras [58].

É importante destacar que da dependência tecnológica originam-se o risco de "l*ock-in*" e os custos de longo prazo. Os contratos de longo prazo (como os do SERPRO, 10 anos com o Google) e a integração profunda com ecossistemas proprietários podem gerar um efeito de "*lock-in*" . Uma vez que os sistemas governamentais estejam rodando sobre as

plataformas da AWS, Google ou Oracle, migra-los no futuro pode se tornar proibitivo. A conta final, incluindo a manutenção da expertise técnica dentro das estatais para gerenciar ambientes cada vez mais complexos, precisa ser cuidadosamente avaliada ao longo do tempo.

Também cumpre considerar a complexidade de governança e integração inerente a este modelo, pois a existência de múltiplos fornecedores (AWS, Google, Huawei, Oracle) e duas estatais operando (Serpro e Dataprev) exige uma governança de alto nível para garantir a interoperabilidade, a padronização de serviços e a eficiência de custos, evitando a criação de "ilhas tecnológicas" soberanas, mas desconectadas entre si . O MGI tem atuado como órgão central para coordenar essa orquestração, definindo preços máximos e diretrizes, mas há de se reconhecer que  o desafio operacional é significativo.

A Nuvem de Governo representa um avanço institucional ao conciliar, de forma pragmática, a urgente modernização da infraestrutura de TI do Estado com a necessidade estratégica de proteger dados sensíveis sob jurisdição nacional. Sua principal vantagem reside na garantia de soberania formal, pois ao tentar assegurar a residência dos dados em território brasileiro e a operação por servidores públicos, o modelo oferece proteção contra ingerências externas e fortalece a conformidade com a LGPD. No entanto, existem fragilidades substanciais em sua dimensão material. A dependência crítica das plataformas e softwares das Big Techs, a ausência de cláusulas robustas de transferência tecnológica e o risco de captura dos interesses públicos pela lógica comercial das parceiras estrangeiras comprometem o ideal de autonomia plena. Em síntese, a nuvem de governo constitui um passo necessário, mas insuficiente para a soberania digital porque avança no controle dos dados, mas permanece refém da tecnologia alheia, evidenciando que a verdadeira independência exigirá, no longo prazo, investimentos consistentes em capacitação própria e desenvolvimento nacional de infraestruturas críticas [58].

Em se tratando de infraestruturas críticas, convém ressaltar que uma Política Nacional de Data Centers, foi lançada em consulta pública pelo Ministério das Comunicações (MCom) em agosto de 2025, visando estruturar o setor com foco em sustentabilidade, conectividade e soberania digital. A iniciativa busca atrair investimentos, incentivar o uso de energia renovável e definir padrões técnicos de qualidade, integrando-se à Política Nacional de Cibersegurança e também à Estratégia Nacional de IA.

### *G. Panorama  Internacional*

A análise da soberania de dados em nuvem, com foco em duas iniciativas no cenário internacional, ilustra como essa não é uma questão meramente técnica, mas uma necessidade inserida em um complexo jogo de leis, geopolítica e poder econômico.

De um lado, no contexto norte-americano, temos o Cloud Act, lei que permite que autoridades dos EUA requisitem dados armazenados por provedores de serviços sujeitos à jurisdição americana, independentemente da localização física dos servidores e a Foreign Intelligence Surveillance Act (FISA), lei que estrutura a vigilância de inteligência estrangeira nos Estados Unidos. Tais leis configuram-se no principal exemplo de conflito de soberania, pois mesmo que uma empresa contrate uma nuvem soberana com dados em território nacional, se o provedor for americano (AWS, Google, Microsoft, Oracle), a Cloud Act pode obrigá-la a entregar os dados ao governo dos EUA, contornando a legislação local [59]. A FISA, juntamente com o Cloud Act, representam elementos críticos de tensão com a soberania de dados, pois a jurisdição americana prevalece sobre a localização física dos servidores, impondo limites à capacidade de provedores americanos de oferecerem genuína soberania de dados a clientes estrangeiros [60].

Do outro lado, no contexto europeu, temos o GAIA-X como uma iniciativa estratégica para criar um ecossistema de dados federado, aberto, seguro e interoperável. Seu objetivo é garantir a soberania digital europeia, permitindo que empresas e governos compartilhem dados em um ambiente de confiança, sem depender exclusivamente de provedores extracomunitários. Propõe um conjunto de regras e padrões comuns (uma espécie de "selo") para que diferentes provedores de nuvem (europeus ou não) possam se conectar de forma transparente, garantindo ao usuário o controle total sobre seus dados e evitando o *lock-in* [61].

O projeto busca oferecer uma alternativa ao domínio dos grandes provedores de nuvem não-europeus (as Big Techs americanas e chinesas, chamadas de hyperscalers), permitindo que empresas, governos e cidadãos europeus mantenham o controle sobre seus dados, onde eles são armazenados e como são processados. A ideia é criar um ambiente de confiança que promova a inovação, permitindo o compartilhamento seguro de dados entre setores e países, e assegure a conformidade com a rigorosa legislação europeia de proteção de dados (GDPR) para evitar a dependência tecnológica

de um único provedor estrangeiro, fomentando um mercado de nuvem mais competitivo e plural na Europa [62]. Portanto, compreender esse pano de fundo global é relevante para avaliar, com realismo, as potencialidades e os limites da estratégia brasileira.

## III. METODOLOGIA

Esta pesquisa é de natureza aplicada, voltada à geração de conhecimento para a solução de problemas práticos relacionados à contratação de serviços de nuvem pelo Governo Federal, com ênfase na garantia da soberania de dados e na conformidade com a LGPD. Adota um delineamento misto, combinando procedimentos qualitativos e quantitativos para uma compreensão abrangente do fenômeno investigado e caracteriza-se como exploratória e descritiva, pois busca identificar e categorizar lacunas contratuais, bem como descrever o estado da arte das contratações públicas de nuvem no âmbito federal. A fundamentação teórica foi construída contemplando fontes acadêmicas, tal como artigos indexados em bases de pesquisa (Research Gate, Google Scholar, Capes CAFe, Web of Science e Scielo), focando prioritariamente nas publicações dos últimos 6 anos, além de fontes técnicas e normativas consagradas (NIST e ISO/IEC 27001), relatórios técnicos de provedores de nuvem, publicações de órgãos de controle e a legislação de regência relacionada ao tema.

De forma simples e objetiva, em uma pesquisa, os "instrumentos de análise" são as ferramentas, técnicas ou métodos utilizados pelo pesquisador para processar, interpretar e extrair significado dos dados brutos que ele coletou. Neste trabalho, o arcabouço normativo fundamentou a elaboração de dois instrumentos de análise que foram utilizados para avaliar contratos de nuvem do governo federal e, neste caso, os contratos figuram como sendo as"unidades de análise".

### *A. Instrumentos de Análise*

Considerando o que a doutrina e a prática regulatória têm apontado [8, 10, 61, 62] , o primeiro instrumento de análise está representado na Tabela VI, que registra as maiores dificuldades para garantia da conformidade com LGPD na nuvem e o desafio que isso representa para o governo.

*Tabela VI – Desafios do governo para conformidade com a LGPD na nuvem*

| Exigência da LGPD | Dificuldade | Desafio para o Governo |
|---|---|---|
| Responsabilidades de Controlador e Operador (Arts. 5º, VII e VIII; Art. 39) | Definição difusa de papéis. Em arquiteturas de nuvem (IaaS, PaaS, SaaS), a linha entre as responsabilidades do controlador (Governo) e do(s) operador(es) torna-se fluida e técnica. O controlador precisa provar que gerencia ativamente o processamento. | O governo, como controlador final, precisa mapear, documentar e auditar uma cadeia de responsabilidade que pode incluir o cloud broker público e o provedor global. Provar esse controle operacional efetivo sobre um serviço gerenciado por terceiros é um desafio probatório constante. |
| Segurança da Informação (Art. 46) | Falta de transparência e auditoria limitada. A LGPD exige medidas adequadas ao risco específico dos dados. Dados governamentais têm risco muito elevado. A dificuldade está em auditar de forma independente as camadas profundas da infraestrutura do provedor, que são opacas por design. | A segurança torna-se uma questão de confiança delegada com responsabilidade retida. Qualquer incidente gera responsabilidade objetiva do governo. Evidenciar que fez "tudo ao seu alcance" exige cláusulas contratuais de altíssimo nível e direitos de auditoria difíceis de negociar. |
| Transferência Internacional de Dados | Ponto Mais Crítico e Intrincado. Em uma arquitetura global dinâmica, os dados são replicados/movidos entre data centers globalmente, sem notificação em tempo real. O acesso por autoridades estrangeiras \|(leis como o US Cloud Act) pode obrigar o provedor a entregar dados ao governo do seu país de origem, independentemente da localização física. | Cria um conflito de soberania insustentável. Dados estratégicos (saúde, defesa) ficam expostos a jurisdições estrangeiras. A contratação via cloud broker nacional não resolve este problema se a infraestrutura final for do provedor global. O governo perde o controle jurisdicional efetivo. |
| Transparência e Direitos dos Titulares (Capítulo III) | Execução prática dos direitos. Garantir direitos (acesso, exclusão, portabilidade) em uma infraestrutura complexa e multi jurisdicional é tecnicamente árduo. O | Para atender a pedidos no prazo legal (15 dias), o governo precisa de canais e processos integrados com o cloud broker e o provedor final. Garantir que uma exclusão de dados se |

| | | |
|---|---|---|
| | controlador depende da cooperação e ferramentas do operador. | reflita em todas as réplicas e backups globais pode não ser tecnicamente viável ou previsto no contrato. |

*Fonte: Elaborado pelo autor*

A análise do arcabouço normativo, com ênfase na IN GSI/PR nº 5/2021 [52], na Portaria SGD/MGI nº 5.950/2023 [54] e na IN GSI/PR nº 8/2025 [54], permitiu identificar 28 cláusulas essenciais para contratações de nuvem no governo federal. Essas cláusulas foram relacionadas a pilares da soberania de dados (localização, controle jurídico, controle operacional e imunidade) e a princípios da LGPD (finalidade, adequação, segurança e prevenção), culminando no segundo instrumento de análise utilizado nesta pesquisa, a Matriz de Requisitos Contratuais (MRC), representada na Tabela VII.

*Tabela VII – Matriz de Requisitos Contratuais (MRC)*

| Id | Cláusula | Pilar Soberania | Princípio LGPD | Fundamento |
|---|---|---|---|---|
| C1 | Vedar expressamente o armazenamento ou processamento de dados em países não autorizados pelo Comitê de Segurança da Informação do órgão. | Localização | Finalidade | IN 5/2021, art. 8º, I |
| C2 | Eleger o foro da Justiça Federal ou do Distrito Federal da sede do órgão contratante como único competente, com aplicação exclusiva da legislação brasileira | Controle Jurídico | Finalidade | IN 5/2021, art. 11, I |
| C3 | Proibir expressamente o uso de informações do órgão pelo provedor para propaganda, otimização de mecanismos de inteligência artificial ou qualquer uso secundário não autorizado | Controle Operacional | Finalidade | IN 5/2021, art. 19, III |
| C4 | Prever termo de confidencialidade que impeça o provedor de usar, transferir e liberar dados para empresas nacionais, transnacionais, estrangeiras, países e governos estrangeiros | Imunidade | Finalidade | IN 5/2021, art. 19, I |
| C5 | Para informações classificadas (reservadas ou secretas), exigir data centers exclusivamente em território nacional, vedada réplica ou backup no exterior | Localização | Adequação | IN 8/2025, art. 4º |
| C6 | Definir claramente os papéis de controlador e operador, a finalidade do tratamento, a obrigação de sigilo e os procedimentos para comunicação de violações | Controle Jurídico | Adequação | IN 5/2021, art. 11, I |
| C7 | Exigir identidade federada com tecnologia single sign-on (SSO) e autenticação multifator (MFA) para acessos críticos, vedado o acesso direto do provedor ao ambiente de autenticação do órgão | Controle Operacional | Adequação | IN 5/2021, art. 13 |
| C8 | Exigir que a política de segurança da informação do provedor esteja em conformidade com a legislação brasileira | Imunidade | Adequação | IN 5/2021, art. 19, IV |
| C9 | Exigir que a infraestrutura do provedor atenda aos requisitos e níveis de qualidade da norma ABNT NBR ISO/IEC 22.237-1:2023 | Localização | Segurança | Portaria 5.950, item 2.1, "h" |
| C10 | Assegurar à Administração o direito de realizar auditorias independentes nos sistemas, controles e instalações do provedor, inclusive in loco | Controle Jurídico | Segurança | IN 5/2021, art. 8º, III; Portaria 5.950, item 1.4 |
| C11 | Exigir criptografia em repouso e em trânsito. Para informações classificadas, as chaves criptográficas devem ser gerenciadas exclusivamente pelo órgão (BYOK), com uso de algoritmos de Estado | Controle Operacional | Segurança | IN 5/2021, art. 3º, IV e V; IN 8/2025 |
| C12 | Estabelecer prazo máximo (ex: 24h) para o provedor notificar a Administração sobre qualquer incidente de segurança, detalhando o ocorrido, as medidas tomadas e, se envolver dados pessoais, apoiar a comunicação à ANPD e aos titulares | Imunidade | Segurança | IN 5/2021, art. 8º, V; LGPD, art. 48; Portaria 5.950, item 2.1 |
| C13 | Para informações classificadas, exigir infraestrutura física dedicada, sem compartilhamento com outros clientes | Localização | Prevenção | IN 8/2025, art. 7º, IV |

| Id | Cláusula | Pilar Soberania | Princípio LGPD | Fundamento |
|---|---|---|---|---|
| C14 | Condicionar qualquer subcontratação à prévia autorização da Administração, estendendo a toda a cadeia de fornecedores as mesmas obrigações de proteção de dados, segurança e confidencialidade | Controle Jurídico | Prevenção | IN 5/2021, art. 8º, II |
| C15 | Obrigar o provedor a fornecer todos os dados da Administração em formato aberto e estruturado ao final da vigência, garantindo a portabilidade como direito do titular (LGPD, art. 18, V) | Controle Operacional | Prevenção | IN 5/2021, art. 11, VII; Portaria 5.950, art. 4º, III |
| C16 | Para informações classificadas, exigir as certificações ABNT NBR ISO/IEC 27001, 27017, 27018, 27701 e 22237 | Imunidade | Prevenção | IN 8/2025, art. 7º, II |
| C17 | Prever custos de saída (egress) pré-definidos e não abusivos, evitando obstáculos à soberania na escolha de novos fornecedores | Controle Operacional | Prevenção | IN 5/2021, art. 11, VII |
| C18 | Prever plano detalhado de transição, contemplando cronograma, formato dos dados, apoio técnico do provedor na migração e obrigação de eliminação segura dos dados após a migração | Controle Operacional | Prevenção | Portaria 5.950, Anexo I |
| C19 | Obrigar o provedor a fornecer informações técnicas detalhadas (fluxo de dados, subcontratação, medidas de privacidade) para subsidiar o RIPD, ou apresentar seu próprio RIPD para validação | Controle Jurídico | Prevenção | IN 5/2021, art. 11, II |
| C20 | Conter cláusula ou anexo detalhando a matriz de responsabilidades entre as partes, conforme o modelo de serviço contratado (IaaS, PaaS, SaaS), especificando as obrigações de cada parte | Controle Operacional | Adequação | IN 5/2021, art. 7º, III e IV |
| C21 | Definir critérios e periodicidade para aplicação de atualizações de segurança pelo provedor | Controle Operacional | Segurança | IN 5/2021, art. 12, I |
| C22 | Garantir a exclusividade de direitos do órgão sobre todas as informações tratadas durante o período contratado, incluídas eventuais cópias disponíveis, como backups de segurança | Controle Jurídico | Finalidade | IN 5/2021, art. 19, II |
| C23 | Prever a devolução integral dos dados, informações e sistemas sob custódia do provedor ao órgão contratante ao término do contrato | Controle Operacional | Prevenção | IN 5/2021, art. 19, V |
| C24 | Obrigar o provedor a eliminar, ao término do contrato, qualquer dado, informação ou sistema do órgão sob sua custódia, observada a legislação que trata da obrigatoriedade de retenção de dados | Controle Operacional | Prevenção | IN 5/2021, art. 19, VI |
| C25 | Garantir o direito ao esquecimento para dados pessoais, conforme art. 16 da Lei nº 13.709/2018 (LGPD) | Controle Jurídico | Prevenção | IN 5/2021, art. 19, VII |
| C26 | Para informações classificadas, exigir credenciamento de segurança de todas as pessoas com acesso à infraestrutura | Controle Operacional | Segurança | IN 8/2025, art. 7º, VIII |
| C27 | Para informações classificadas, o contrato deve ser formalizado como sigiloso, nos termos do Decreto nº 7.845/2012 | Controle Jurídico | Prevenção | IN 8/2025, art. 9º, I |
| C28 | Nos casos de contratação de serviço de integração (broker), obrigar a disponibilização de uma estrutura exclusiva de contas nos provedores de nuvem em nome do órgão contratante, garantindo a propriedade e o controle dos dados | Controle Operacional | Prevenção | Portaria SGD/MGI 5.950 |

*Fonte: Elaborado pelo autor*

*B. Unidades de Análise*

Uma amostra, composta por 13 contratos de serviços de nuvem celebrados por órgãos da Administração Pública Federal entre 2019 e 2026, foi selecionada a partir dos dados disponíveis no Portal da Transparência e Portal Nacional de Contratações Públicas (PNCP). Essa amostra foi complementada por informações solicitadas diretamente aos órgãos na

forma de pedidos de informação viabilizados pela Lei de Acesso à Informação (LAI). A escolha procurou incorporar contratos relativos aos três modelos de serviços em nuvem (IaaS, PaaS, SaaS), bem como diferentes modalidades de contratação (nuvem pública, nuvem de governo e cloud brokerage), abrangendo ministérios, autarquias e conselhos federais, conforme indicado na Tabela VIII.

*Tabela VIII – Contratos de Nuvem do Governo Federal*

| Órgão | Nº Contrato | Ano |
|---|---|---|
| Conselho Administrativo de Defesa Econômica (CADE) | 07/2019 (PRIMESYS) | 2019-2021 |
| Ministério do Planejamento (MP) | 40/2019 (CLARO) | 2019-2022 |
| Ministério de Gestão e Inovação (MGI) | 65/2021 (SERPRO) | 2021-2024 |
| Ministério da Economia (ME) | 17/2021 (DATAPREV) | 2021-2023 |
| Fundo Nacional de Desenvolvimento da Educação (FNDE) | 90064/2023 (SERPRO) | 2023-2026 |
| Ministério da Educação (MEC) | 23000.002519/2024-11 (SERPRO) | 2024-2027 |
| Agência Nacional de Águas (ANA) | 19/2024 (SERPRO) | 2024-2027 |
| Ministério de Gestão e Inovação (MGI) | 65/2025 (SERPRO) | 2025-2030 |
| Ministério da Agricultura (MAPA) | 45/2025 (DATAPREV) | 2025-2027 |
| Ministério da Educação (MEC) | Nº 16//2025 (DATAPREV/TELEBRAS/SERPRO) | 2025-2030 |
| Conselho Federal de Fisioterapia E Terapia Ocupacional (COFFITO) | 53/2025 (SERPRO) | 2025-2026 |
| Ministério da Educação (MEC) | 17/2025 (/TELEBRAS) | 2025-2030 |
| Ministério da Fazenda (MF) | 18220.001182/2025-73 (SERPRO) | 2026-2036 |

*Fonte: Elaborado pelo autor*

*C. Procedimentos de Análise*

A análise documental combinou procedimentos qualitativos e quantitativos. Quanto à abordagem qualitativa, aplicou-se a técnica de análise dirigida de conteúdo, na qual os instrumentos de análise elaborados (Tabelas VI e VII) funcionaram como um protocolo de verificação estruturado. Cada contrato foi examinado para avaliar a conformidade com a LGPD e também identificar a presença, localização e redação das 28 cláusulas da Matriz de Requisitos Contratuais. Em sua natureza quantitativa, foi definida uma escala ordinal para mensuração de aderência. Na inspeção dos contratos, para cada cláusula da MRC (Tabela VII), atribuiu-se uma pontuação conforme a classificação da Tabela IX.

*Tabela IX– Pontuação para aferição da aderência à MRC.*

| Pontuação | Classificação | Critério |
|---|---|---|
| 0 | Ausente | Cláusula não consta no contrato |
| 1 | Parcial | Cláusula consta, mas com redação genérica ou insuficiente |
| 2 | Pleno | Cláusula consta com redação adequada às exigências normativas |
| NA | Não se Aplica | Cláusula direcionada a situações específicas não contempladas no contrato |

*Fonte: Elaborado pelo autor*

De acordo com a pontuação obtida por cada contrato, foi calculado o percentual de aderência à MRC, conforme indicado na Equação 1. A pontuação máxima possível corresponde ao somatório dos valores máximos (2, Pleno) para cada cláusula aplicável, desconsideradas aquelas classificadas como "NA".

$$\text{Aderência (\%)} = \frac{\text{Pontuação Total Alcançada}}{\text{Pontuação Máxima Possível}} \times 100$$

*Equação 1 – Cálculo para aferição da aderência à MRC*
*Fonte: Elaborado pelo autor*

As análises foram registradas de forma padronizada, conforme exemplificado na Tabela X, com descrição textual da localização das cláusulas e avaliação qualitativa da redação, permitindo a categorização das fragilidades e identificação de boas práticas.

*Tabela X – Exemplo da Padronização Utilizada para a Análise dos Contratos*

| **CONSELHO ADMINISTRATIVO DE DEFESA ECONÔMICA (CADE)** | | **CONTRATO:** Nº 07/2019 (PRIMESYS S/A) **ANO:** 2019-2021 | **Aderência** 36 / 50 = **72,0%** | |
|---|---|---|---|---|
| **Cláusula** | **Descrição** | **Localização** | **Análise** | **Pontos** |
| C01 | Vedar armazenamento/processamento em países não autorizados pelo CSI | Termo de Referência (TR), item 5.1.8 e item 6.1.23; Contrato, Cláusula 16.6.1 | Plena. O TR (5.1.8) exige que os serviços sejam executados "em território nacional... incluindo replicação e cópias de segurança (backups)". O item 6.1.23 reforça a proibição de replicar dados fora do território brasileiro. O Contrato (16.6.1) prevê multa para o descumprimento. Embora não mencione o CSI, a vedação ao processamento fora do Brasil é explícita e abrangente. | 2 |
| C02 | Eleger foro da Justiça Federal/DF com aplicação exclusiva da lei brasileira | Contrato, Cláusula Vigésima Segunda (22ª) | Plena. O contrato é explícito ao eleger o "Foro da Seção Judiciária de Brasília - DF - Justiça Federal". A aplicação da legislação brasileira (Lei 8.666/93, etc.) é a base de todo o instrumento. | 2 |
| ... | ... | ... | ... | ... |
| C28 | Nos casos de contratação de serviço de integração (broker), obrigar a disponibilização de uma estrutura exclusiva de contas nos provedores de nuvem em nome do órgão contratante, garantindo a propriedade e o controle dos dados | TR, item 5.1.3 e Contrato, item 1.3 | Plena. O TR (5.1.3) é explícito: "A CONTRATADA deverá disponibilizar uma conta no provedor em nome da CONTRATANTE". O item 5.1.3.1 ainda permite que a contratante delegue acesso à contratada. A propriedade da conta e, por extensão, o controle sobre os dados provisionados nela, é garantida ao órgão. | 2 |
| | | | **Total** | 36 |

*Fonte: Elaborado pelo autor*

Os resultados foram consolidados na Tabela XI, permitindo a comparação entre contratos de diferentes períodos, fornecedores e modelos de contratação. Os dados quantitativos (percentuais de aderência), conforme a Equação 1, foram analisados em conjunto com as anotações qualitativas extraídas da análise de conteúdo, permitindo a identificação de tendências evolutivas, padrões de conformidade e lacunas recorrentes. A partir dessa integração, foram categorizadas as principais fragilidades contratuais e estabelecidas correlações com os desafios teóricos identificados neste estudo. Os achados foram então discutidos à luz do referencial teórico e revisão da literatura, culminando na proposição de aprimoramentos aos marcos contratuais e de governança para contratação de serviços em nuvem.

## IV. RESULTADOS E DISCUSSÕES

Conforme explanado na Seção III, utilizando a MRC, foram realizadas as análises dirigidas de conteúdo sobre 13 contratos do governo federal. A Tabela XI está ordenada considerando o ano de início de vigência dos contratos e indica o percentual de aderência à Matriz de Requisitos Contratuais, conforme a pontuação obtida.

*Tabela XI – Aderência dos Contratos à MRC*

| Órgão | Nº Contrato | Ano | Aderência |
|---|---|---|---|
| Conselho Administrativo de Defesa Econômica (CADE) | 07/2019 (PRIMESYS) | 2019-2021 | 72% |
| Ministério do Planejamento (MP) | 40/2019 (CLARO) | 2019-2022 | 58% |
| Ministério de Gestão e Inovação (MGI) | 65/2021 (SERPRO) | 2021-2024 | 70% |

| | | | |
|---|---|---|---|
| Ministério da Economia (ME) | 17/2021 (DATAPREV) | 2021-2023 | 37,5% |
| Fundo Nacional de Desenvolvimento da Educação (FNDE) | 90064/2023 (SERPRO) | 2023-2026 | 58,7% |
| Ministério da Educação (MEC) | 23000.002519/2024-11 (SERPRO) | 2024-2027 | 83,3% |
| Agência Nacional de Águas (ANA) | 19/2024 (SERPRO) | 2024-2027 | 76% |
| Ministério de Gestão e Inovação (MGI) | 65/2025 (SERPRO) | 2025-2030 | 89,58% |
| Ministério da Agricultura (MAPA) | 45/2025 (DATAPREV) | 2025-2027 | 81,30% |
| Ministério da Educação (MEC) | Nº 16//2025 (DATAPREV/TELEBRAS/SERPRO) | 2025-2030 | 74% |
| Conselho Federal de Fisioterapia E Terapia Ocupacional (COFFITO) | 53/2025 (SERPRO) | 2025-2026 | 82,0% |
| Ministério da Educação (MEC) | 17/2025 (/TELEBRAS) | 2025-2030 | 72% |
| Ministério da Fazenda (MF) | 18220.001182/2025-73 (SERPRO) | 2026-2036 | 87% |

*Fonte: Elaborado pelo autor*

A apreciação qualitativa realizada no referencial teórico deste estudo associada à análise dirigida de conteúdo aplicada aos contratos de serviços de nuvem do Governo Federal, celebrados entre 2019 e 2026, revela um cenário de avanços graduais, mas também de fragilidades estruturais que comprometem a efetividade da soberania de dados e a conformidade com a LGPD. Os resultados são aqui apresentados e discutidos à luz dos objetivos específicos propostos.

*A. Evolução da Aderência e Lacunas Contratuais Persistentes*

A aplicação da Matriz de Requisitos Contratuais (MRC) evidencia uma trajetória de melhoria nos índices de conformidade ao longo do período analisado. Contratos mais antigos, como o do Ministério do Planejamento (MP-40/2019 – 58%) e, de forma mais crítica, o do Ministério da Economia (ME-17/2021 – 37,5%), apresentam os menores percentuais, refletindo um período anterior à consolidação de normativos como a IN GSI/PR nº 5/2021 [51]. Em contraste, contratações recentes, como a do Ministério da Gestão e da Inovação (MGI-65/2025 – 89,58%) e do Ministério da Educação (23000.002519/2024-11 – 83,3%), demonstram uma incorporação mais sistemática das exigências legais e técnicas [20, 52, 54]. Para fins de clareza, as referências entre parênteses que serão apresentadas a partir de agora, como por exemplo “(C10)”, referem-se às cláusulas da MRC que constam da Tabela VII.

A análise referente ao contrato mais recente, do Ministério da Fazenda (MF-18220.001182/2025-73), celebrado em 2026 com o SERPRO com valor superior a R$ 900 milhões, revela um interessante nível de conformidade, alcançando 87% de aderência à MRC. Este contrato não apenas consolida as boas práticas observadas nos instrumentos anteriores, mas também incorpora inovações significativas, como a definição explícita dos papéis de Controlador e Operador (C06), a estipulação de prazo objetivo de 24 horas para notificação de incidentes de segurança (C12) e a expressa vedação ao uso de dados para treinamento de inteligência artificial fora do escopo contratual (C03), uma cláusula prospectiva que dialoga diretamente com os riscos associados ao capitalismo de vigilância [1]. A menção à Resolução CD/ANPD nº 19/2024 [61] demonstra, ainda, uma incorporação tempestiva das normas complementares da Autoridade Nacional de Proteção de Dados, evidenciando um amadurecimento institucional na estruturação dos instrumentos contratuais.

No entanto, a persistência de contratos com pontuação intermediária mesmo em 2025 (ex: MEC-17/2025 – 72%) indica que a internalização das normas pelos órgãos contratantes ainda é desigual e que determinados requisitos são sistematicamente negligenciados, configurando lacunas contratuais críticas apresentadas na Tabela XII.

*Tabela XII – Lacunas Contratuais Frequentes*

| **Lacunas Contratuais** |
|---|
| **Invisibilidade dos Custos de Saída** (C17). A ausência de previsão sobre custos de *egress* é a falha mais recorrente. Nenhum dos contratos recentes aborda o tema, o que contrasta com a boa prática identificada no contrato do CADE-2019, que previa transferência "sem custo adicional". Essa omissão institucionaliza o risco de aprisionamento tecnológico *(vendor lock-in*) [50], permitindo que, ao final do contrato, o provedor inviabilize a troca de fornecedor mediante a cobrança de valores abusivos para a devolução dos dados. Trata-se de um obstáculo direto à soberania na escolha futura e à livre concorrência. |

| |
|---|
| **Generalidade na Notificação de Incidentes** (C12). A maioria dos contratos utiliza o termo vago "imediatamente" para obrigar a notificação de incidentes de segurança. A estipulação de prazos objetivos, como as 24h previstas no contrato do MGI (nº 65/2025) e MEC (nº 17/2025), é uma exceção. Essa imprecisão compromete a capacidade da Administração de responder prontamente a violações de dados pessoais, descumprindo o dever de comunicação à ANPD e aos titulares, conforme preconiza o art. 48 da LGPD [6]. |
| **Incompletude na Definição de Papéis** (C06). Apesar da menção à LGPD ser comum, a definição formal e explícita dos papéis de Controlador e Operador (C06) ainda é superficial em muitos instrumentos. Contratos que atingem a pontuação máxima nesse critério, o fazem por meio de anexos específicos de LGPD que detalham essas responsabilidades. A ausência dessa clareza, conforme alerta a literatura, gera zonas cinzentas de responsabilidade e dificulta o exercício do controle determinante pelo Estado, especialmente em modelos de serviço complexos como IaaS, PaaS e SaaS [11, 62, 48]. |
| **Subutilização do RIPD** (C19). A exigência de informações para subsidiar o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) é completamente ignorada em todos os contratos. Mesmo aqueles com cláusulas de LGPD bem desenvolvidas não mencionam o RIPD, revelando que a Administração Pública ainda não internalizou essa ferramenta fundamental de governança de riscos à privacidade, conforme previsto na LGPD e na IN 5/2021 [6, 52]. A persistência desta lacuna, mesmo no contrato mais recente analisado (janeiro de 2026), sugere que sua superação depende não apenas da evolução natural dos modelos contratuais, mas de uma intervenção normativa sistêmica que a torne obrigatória. |
| **Ausência de Normas Técnicas Específicas** (C09). A exigência de que a infraestrutura do provedor atenda à norma ABNT NBR ISO/IEC 22.237-1:2023 (norma de data center) é um ponto cego em praticamente todos os contratos. Nenhum dos instrumentos analisados faz menção a essa norma, o que sugere um desconhecimento ou uma priorização de outras certificações, como as ISO 27001 e 27017. |

*Fonte: Elaborado pelo autor*

Em tese, muitas destas deficiências contratuais poderiam ser supridas pelas disposições dos termos de serviço ofertados pelas Big Techs, os CDPAs (Cloud Process Data Addendum) mencionados anteriormente neste estudo. A relação entre CDPAs, o modelo de cloud brokerage e as lacunas observadas merece uma discussão um pouco mais aprofundada. Embora os CDPAs representem o padrão de mercado para a formalização da responsabilidade compartilhada entre provedores e clientes no setor privado [45, 46], sua adoção direta nos contratos da Administração Pública Federal mostrou-se inviável. A análise dos 13 instrumentos revelou que, quando mencionados, os CDPAs são sistematicamente substituídos ou complementados por anexos específicos elaborados pelos brokers estatais (SERPRO e DATAPREV) ou pelos próprios órgãos contratantes. Essa substituição decorre de três incompatibilidades fundamentais. A primeira é o conflito de foro e jurisdição, pois os CDPAs padrão elegem foros estrangeiros e submetem controvérsias à legislação desses países [45, 46], em frontal desacordo com o art. 11 da IN GSI/PR nº 5/2021, que exige a eleição do foro da Justiça Federal ou do Distrito Federal (C2). A segunda é a ausência de cláusulas de soberania nacional, verifica-se que os CDPAs não contemplam vedações a países não autorizados pelo CSI (C1), nem exigências de identidade federada com SSO e MFA (C7), requisitos impostos pela legislação brasileira. A terceira é a omissão quanto aos custos de saída (egress), os CDPAs são silentes sobre custos de egress (C17) e formatos abertos de dados (C15), lacunas que, ao serem aceitas, consolidariam o risco de aprisionamento tecnológico [50]. Esses instrumentos foram desenhados para fidelizar o cliente, não para garantir sua autonomia futura. O governo, ao aceitar os CDPAs sem adaptação, estaria renunciando a prerrogativas essenciais à soberania digital. O modelo de cloud brokerage estatal atuou como um filtro institucional para contornar essas incompatibilidades. Ao centralizar as contratações, SERPRO e DATAPREV elaboraram anexos específicos que traduziram as exigências da IN GSI/PR nº 5/2021 e da LGPD em obrigações contratualmente exigíveis dos provedores de serviços em nuvem.

No entanto, mesmo esse modelo não suprimiu integralmente as lacunas, pois requisitos como custos de saída (C17) e RIPD (C19) permanecem ausentes, indicando que as adaptações operadas pelos brokers priorizaram a conformidade normativa imediata, mas não enfrentaram as assimetrias estruturais de poder que perpetuam o risco de *lock-in* e a subutilização de instrumentos de governança proativa. Esses achados corroboram a literatura que aponta que a soberania de dados e conformidade com a LGPD nos contratos administrativos vai além da mera inclusão de cláusulas genéricas, exigindo detalhamento operacional e a definição inequívoca de responsabilidades para mitigar riscos jurídicos e de segurança da informação. Como alertam Doneda e Almeida [8], a efetividade da proteção de dados depende de sua concretização em mecanismos operacionais, enquanto Oliveira et al. [10] também se alinham nesta direção e destacam a necessidade de governança ativa no setor público. Essa visão é reforçada pelos achados do TCU sobre riscos contratuais em serviços de nuvem [50], visto que já em 2015 registravam-se estimativas imprecisas de custos, incluindo custos de saida, assim como os riscos de dependência do fornecedor e a demora dos provedores para detecção e correção de vulnerabilidades e problemas de segurança.

*B. Avanços, Limitações e o Dilema da Soberania Real em Nuvem Pública e Nuvem de Governo*

Um estudo sobre os data centers no país, realizado por Marques e Oliveira [63], permite evidenciar a elevada dependência tecnológica e de capital estrangeiro. Conforme registrado pelos autores, 69% dos data centers no Brasil são controlados por 16 empresas, sendo 14 delas multinacionais (principalmente dos EUA). Neste cenário de dependência tecnológica estrutural, que compromete a soberania digital, tecnológica e de dados, o Brasil depende de componentes de hardware e software importados (servidores, roteadores, sistemas de refrigeração, middleware, entre outros) e de serviços de nuvem estrangeiros. A produção nacional limita-se a itens de baixa complexidade, como sistemas de segurança e distribuição de energia [63]. Desta forma, verifica-se a parceria de empresas públicas nacionais, como SERPRO, com Big Techs (Google, Microsoft, AWS, Huawei e Oracle) para o fornecimento de serviços de nuvem pública para o governo federal, e esta iniciativa tem sido alvo de algumas críticas. Tendo sido criado para a prestação de serviços estratégicos de TI aos órgãos da União, o SERPRO, ao firmar essas parcerias para oferta de serviços em nuvem pública, parece distanciar-se dos requisitos de soberania digital e soberania de dados, submetendo o controle das infraestruturas digitais a essas empresas e possibilitando que diversos órgãos de direito público interno da esfera federal contratem serviços de armazenamento em nuvem nos quais a estatal atua como intermediária [58]. Esta prática deve ser apreciada criticamente pois na Lei 5.615/1970, que cria o SERPRO, há vedação explícita sobre a subcontratação de outras empresas para a prestação direta de serviços estratégicos de TI, todavia é o art. 28 (§3º, II e §4º) da Lei das Estatais (Lei 13.303/2016) que ampara diretamente as parcerias comerciais do Serpro com as Big Techs, através da definição da "oportunidade de negócio", que é uma hipótese que afasta a obrigação legal de licitar, desde que a parceria vise uma vantagem competitiva ou um objetivo de mercado mais amplo, não se limitando a uma simples compra ou prestação de serviços.

Neste cenário onde empresas públicas federais atuam como intermediários (cloud brokers) entre o governo e os grandes provedores de serviços em nuvem pública, o que se verifica é um processo de “captura cognitiva”, um fenômeno em que agentes públicos (gestores, técnicos, formuladores de políticas) passam a internalizar as premissas, os valores e os modelos mentais do setor privado, especialmente das Big Techs, como se fossem naturalmente os melhores ou os únicos possíveis para o Estado. Seus efeitos são sutis e profundos, porque o interesse público estratégico é deslocado não por coerção externa, mas porque os próprios tomadores de decisão já não conseguem enxergar alternativas fora do repertório oferecido pelas grandes empresas de tecnologia. Em suma, captura cognitiva é a colonização das mentes e do imaginário institucional pelo pensamento privado estrangeiro, tornando a subordinação voluntária e invisível. Ela antecede e viabiliza a “captura de agenda”, que indica quais problemas merecem atenção. Assim, os interesses privados passam a moldar as políticas e a atuação do Estado e o interesse público estratégico é gradualmente substituído pela lógica comercial e de parceria com os próprios agentes que poderiam ameaçar a soberania. Essas “capturas” podem ser evidenciadas quando: i) As Big Techs ditam os padrões tecnológicos a serem adotados (ex.: formatos de nuvem, protocolos de IA), ii) A busca por “eficiência” e “modernidade” se equipara à adoção de soluções prontas oferecidas por essas empresas, desincentivando o desenvolvimento de soluções nacionais e iii) O discurso de “soberania digital” é apropriado e esvaziado pelas próprias Big Techs para vender serviços (ex.: Microsoft Cloud for Sovereignty), confundindo a discussão pública [58].

Já a iniciativa da Nuvem de Governo, materializada nos contratos de cloud broker com o SERPRO e a DATAPREV (ex: contratos MGI nº 65/2025 e MAPA nº 45/2025), representa um avanço institucional ao assegurar a soberania formal com a residência dos dados em território nacional e a operação por servidores de empresas públicas. Essa arquitetura mitiga o risco de acesso não autorizado por jurisdições estrangeiras baseado unicamente na localização física dos dados, um ponto crítico em um cenário global onde leis como o Cloud Act dos EUA permitem que autoridades acessem dados de provedores americanos independentemente de sua localização. No entanto, a análise dos contratos e o debate público mais amplo expõem, conforme a Tabela XIII as limitações desse modelo para a soberania material.

*Tabela XIII – Limitações da Nuvem de Governo em relação à Soberania de Dados*

| **Limitações da Nuvem de Governo** |
|---|
| **Dependência Tecnológica Estrutural.** A Nuvem de Governo não elimina a dependência dos softwares, plataformas e ferramentas de gestão das Big Techs. O Brasil adquire o direito de uso dessas tecnologias, mas não detém o controle sobre seu código-fonte, seu desenvolvimento futuro ou sua governança interna. Como alertam os críticos, trata-se de uma "soberania fatiada", onde o controle da camada física (datacenter) não se traduz em autonomia sobre a camada lógica (software). Essa dependência mantém o País suscetível a decisões |

| |
|---|
| unilaterais das corporações estrangeiras e a potenciais vulnerabilidades ou "backdoors" inseridos em seus produtos [13, 66]. |
| **Risco de "Lock-in" e Custos de Longo Prazo**. A opção por contratos de longo prazo (até 10 anos) com integração profunda em ecossistemas proprietários pode gerar um novo tipo de aprisionamento. Isto ilustra de forma paradigmática tanto os benefícios quanto os riscos do modelo de Nuvem de Governo. Por um lado, a longa duração oferece estabilidade e previsibilidade para o planejamento estratégico da infraestrutura de TI do órgão. Por outro, amplifica o risco de aprisionamento tecnológico, especialmente na ausência de cláusulas que prevejam custos de saída e portabilidade irrestrita em formatos abertos. A dependência das plataformas das Big Techs subjacentes, ainda que intermediada pelo SERPRO ou DATAPREV, torna a migração futura um desafio de proporções potencialmente inviabilizadoras, consolidando uma dependência que a própria soberania digital busca evitar. |
| **Exposição ao Arcabouço Legal Estrangeiro**. Apesar da operação por estatais, as Big Techs envolvidas são empresas sediadas em países com legislações de vigilância extraterritorial. O Cloud Act e a Foreign Intelligence Surveillance Act (FISA) podem, em tese, ser usados para coagir essas empresas a fornecerem dados ou criarem mecanismos de acesso, mesmo que os servidores estejam no Brasil. A "camada de criptografia" ou a "conta em nome do cliente" não eliminam esse risco geopolítico fundamental [13, 61, 66]. |

*Fonte: Elaborado pelo autor*

Portanto, a Nuvem de Governo, da forma como está estruturada, mitiga os riscos mais imediatos de acesso direto a dados por governos estrangeiros, mas não constrói, por si só, a autonomia tecnológica e tampouco a soberania digital. Ela troca a dependência da infraestrutura física pela dependência do software e das plataformas, um avanço que, se não for acompanhado de políticas robustas de transferência de tecnologia e fomento à indústria nacional de software, pode consolidar uma nova forma de subordinação digital. O Estado deve investir em capacitação tecnológica própria, mesmo que mais custosa no curto prazo.

A recente descoberta do enorme potencial brasileiro para a exploração de terras raras representa uma oportunidade estratégica para romper com o ciclo de dependência tecnológica apontado no parágrafo anterior. Se o país se limitar a exportar o minério bruto, repetirá o padrão primário-exportador, No entanto, ao condicionar a exploração das terras raras à instalação de plantas de beneficiamento, refino e fabricação de componentes de hardware em território nacional, mediante acordos de transferência de tecnologia com multinacionais, o Brasil pode ascender na cadeia produtiva. Ímãs de terras raras são essenciais para discos rígidos, motores de veículos elétricos, turbinas eólicas e equipamentos de data centers. Dominar esse elo permitiria ao país produzir internamente componentes críticos que hoje importa, reduzindo a vulnerabilidade a sanções ou interrupções de cadeias externas. Assim, as terras raras tornam-se vetor de fomento à indústria nacional de hardware, complementando a soberania digital que a Nuvem de Governo não alcança por si só. De nada adianta controle sobre dados se o substrato físico (servidores, chips, armazenamento) permanecer refém de terceiros. Com políticas industriais robustas, como conteúdo local mínimo (que significa exigir, por lei ou por cláusula contratual em concessões, parcerias ou leilões, que um percentual mínimo dos insumos, componentes, equipamentos ou serviços de um projeto seja fornecido por empresas nacionais) e incentivo à pesquisa e desenvolvimento, o Brasil pode transformar uma commodity em alavanca para autonomia tecnológica.

### *C. O Panorama Internacional e a Imaturidade da Base Legal Nacional*

A análise do cenário internacional revela a imaturidade da estratégia brasileira. Enquanto a União Europeia, por meio do GAIA-X, busca construir um ecossistema de dados federado, baseado em padrões abertos e interoperabilidade, que garanta a soberania digital sem depender exclusivamente de provedores extracomunitários [13], o Brasil optou por um modelo de dependência negociada.

A recente aprovação do Regulamento de Transferência Internacional de Dados pela ANPD (Resolução CD/ANPD nº 19/2024) é um passo crucial para dar segurança jurídica a esses fluxos, estabelecendo cláusulas-padrão contratuais (SCCs) como mecanismo de garantia [65]. Contudo, a efetividade desse instrumento ainda é incerta, pois depende da fiscalização e da capacidade do Estado de monitorar e auditar o cumprimento dessas cláusulas por gigantes tecnológicas globais. Além disso, a Política Nacional de Data Centers, lançada em consulta pública pelo Ministério das Comunicações em 2025, reconhece a infraestrutura de data centers como crítica para a soberania nacional. No entanto, críticos apontam que a política em discussão pode, na prática, aprofundar a subordinação ao oferecer incentivos fiscais para a instalação de centros de dados estrangeiros sem contrapartidas robustas de desenvolvimento tecnológico local e sem uma regulação ambiental e social adequada, repetindo erros observados em outros países.

O debate público e as manifestações de entidades sindicais e acadêmicas evidenciam a percepção de que o Brasil está diante de uma escolha estratégica, que significa aceitar um papel subordinado no ecossistema digital global, ou retomar e atualizar políticas de fomento ao software livre, hardware aberto e à criação de infraestruturas públicas de dados como caminhos para uma soberania digital efetiva [3].

## V. LIMITAÇÕES DA PESQUISA

Embora este trabalho tenha alcançado seus objetivos e produzido contribuições relevantes, é necessário reconhecer suas limitações. Ao se concentrar exclusivamente no Poder Executivo Federal, estados, municípios, Tribunais de Contas, Ministério Público e Poder Judiciário não são considerados e os achados, portanto, não podem ser generalizados para esses entes, cujas realidades contratuais e de governança podem diferir em alguma medida. Os 13 contratos analisados constituem número suficiente para identificar padrões e lacunas recorrentes, mas ainda assim é um numero modesto diante do universo de contratações de nuvem da Administração Pública Federal entre 2019 e 2026. Uma amostra mais ampla poderia revelar variações setoriais ou especificidades não capturadas.

A análise dependeu de documentos obtidos por meio do Portal da Transparência, Portal Nacional de Contratações Públicas e pedidos LAI. Em diversos casos, anexos técnicos, relatórios de *due diligence*, termos aditivos não publicados e os próprios CDPAs não estavam disponíveis ou foram fornecidos de forma incompleta, limitando a profundidade da análise. Convém destacar também que não se realizou uma validação empírica e assim, barreiras práticas de negociação, dificuldades de monitoramento contratual e a efetividade real dos controles de governança foram inferidas exclusivamente da análise documental, sem confirmação direta com os atores envolvidos.

Por fim, quanto ao caráter recente das normas convém destacar que o pouco tempo decorrido desde a publicação de normativos relevantes, como a IN GSI/PR nº 8/2025, Resolução CD/ANPD nº 19/2024 e Portaria SGD/MGI nº 5.950/2023, não permite que seus efeitos sobre as práticas contratuais estejam plenamente consolidados, exigindo observação longitudinal para avaliação de seu impacto efetivo.

## VI. CONCLUSÃO

O governo federal brasileiro trilha uma rota de amadurecimento digital que reflete a tensão entre eficiência e controle soberano. Impulsionada pela política de "nuvem em primeiro lugar", a administração federal inicialmente recorreu a grandes provedores internacionais para processar informações sensíveis e garantir agilidade e redução de custos em nuvens públicas. Essa estratégia, porém, entrou em uma segunda fase com o avanço do arcabouço normativo e a crescente preocupação com segurança da informação e soberania de dados. A resposta a esse novo paradigma foi a consolidação da chamada "Nuvem de Governo". Trata-se de um movimento claro de repatriação, que busca reduzir a dependência de estruturas sediadas no exterior, com a meta de que ao menos 20% dos dados públicos sejam transferidos para esse novo ambiente até 2027 [67, 68], representando uma tentativa de alinhar a transformação digital à proteção das informações do Estado.

Neste contexto, esta pesquisa analisou criticamente a capacidade dos mecanismos de contratação e governança de serviços de nuvem do Governo Federal em garantir a soberania dos dados e a conformidade com a LGPD. A partir da análise documental de 13 contratos e da construção de uma Matriz de Requisitos Contratuais (MRC) alinhada ao arcabouço normativo, foi possível atingir os objetivos propostos e confirmar a hipótese de que existem lacunas significativas nos ajustes celebrados entre o governo federal e os provedores de serviços em nuvem, que comprometem a conformidade com a Lei Geral de Proteção de Dados Pessoais. Também se evidenciou que a estratégia nacional para garantir a soberania de dados mostra-se fragilizada em virtude da dependência significativa de insumos estrangeiros em nossas infraestruturas de tecnologia.

No tocante aos aspectos contratuais, a análise quantitativa e qualitativa revelou que, apesar de uma evolução nos índices de aderência, persistem fragilidades graves. A ausência de previsão de custos de saída (egress), ausência de prazos objetivos para notificação de incidentes, a definição insuficiente dos papéis de controlador e operador e a completa ausência de Relatórios de Impacto à Proteção de Dados Pessoais (RIPD) são os gargalos mais críticos. Essas lacunas criam riscos de aprisionamento tecnológico, comprometem a resposta a violações de dados e enfraquecem a posição do Estado como controlador, em desacordo com os princípios de *accountability* e prevenção da LGPD [6, 50].

Quanto à iniciativa da Nuvem de Governo, é possível reconhecer um avanço formal ao assegurar a localização dos dados e a operação por estatais, mitigando riscos de acesso extraterritorial direto. No entanto, sua arquitetura baseada em plataformas proprietárias de Big Techs estrangeiras não garante a soberania material. Ela mantém uma dependência tecnológica estrutural que expõe o Estado a riscos de *lock-in*, a ingerências indiretas via legislação estrangeira e ao controle limitado sobre o ciclo de vida do software que constitui o núcleo proprietário da plataforma de nuvem (como hipervisores, camadas de gestão de armazenamento, APIs de orquestração e sistemas de telemetria). Esclarece-se que esta limitação não se aplica aos softwares nacionais desenvolvidos pelo governo e instalados sobre a nuvem, cujo ciclo de vida pode ser gerido localmente, mas sim ao ambiente de infraestrutura de nuvem em si, cuja evolução e manutenção profunda permanecem sob controle exclusivo de Big Techs estrangeiras. A soberania neste modelo torna-se inevitavelmente incompleta, pois o governo não detém a última palavra sobre o comportamento, as correções ou o fim de vida do software que governa fisicamente os dados. Do ponto de vista da conformidade com a Lei Geral de Proteção de Dados (LGPD), essa dependência de um núcleo tecnológico proprietário estrangeiro gera riscos concretos e não triviais. Em relação ao art. 46 (dever de segurança), o fato de o Estado não controlar o ciclo de vida do software de infraestrutura impede a correção autônoma de vulnerabilidades, sujeitando os dados pessoais a prazos e prioridades do fornecedor, além disso, a impossibilidade de auditar o código-fonte ou verificar a existência de backdoors torna as medidas de segurança parcialmente opacas, fragilizando a obrigação de adotar salvaguardas aptas a proteger os dados. Quanto ao art. 6º, VIII (princípio da prestação de contas), a arquitetura proprietária inviabiliza a demonstração independente de conformidade, pois o controlador público não pode comprovar, sem depender exclusivamente de declarações da Big Tech, a integridade dos logs de acesso, a ausência de transferências extraterritoriais disfarçadas de telemetria ou a aplicação tempestiva de correções críticas. Essa assimetria informativa expõe o Estado a sanções administrativas e judiciais, uma vez que, nos termos da LGPD, o controlador não se exonera por falta de controle técnico sobre seus prestadores. Assim, a incompletude da soberania não é apenas geopolítica ou tecnológica, ela reverbera diretamente em riscos jurídicos concretos e na dificuldade de se alcançar um nível aceitável de conformidade regulatória.

Em relação à apreciação da base legal e da estratégia nacional, constata-se um nítido contraste com iniciativas como o GAIA-X, que busca autonomia via padrões abertos e interoperabilidade. A ausência de uma política industrial e tecnológica de longo prazo que fomente a produção nacional de software e hardware, aliada a uma regulação que ainda não consegue equilibrar a atração de investimentos estrangeiros com a proteção efetiva da soberania, evidencia a imaturidade do projeto nacional de soberania digital e de dados. Neste contexto, para superar essa imaturidade, o Brasil dispõe de alternativas concretas ancoradas em sua base de recursos naturais estratégicos. A recente descoberta do enorme potencial brasileiro para a exploração de terras raras oferece uma janela de oportunidade que não deve ser desperdiçada na lógica primário-exportadora. Ao condicionar a exploração desses minerais à instalação de plantas de beneficiamento, refino e fabricação de componentes de hardware em território nacional, mediante exigência de conteúdo local mínimo, acordos de transferência de tecnologia com multinacionais e incentivos fiscais vinculados a metas de pesquisa e desenvolvimento, o país pode ascender na cadeia produtiva de bens de alta densidade tecnológica. Tais bens são essenciais para a fabricação de discos rígidos, servidores, sistemas de armazenamento e equipamentos de data centers, e tornam-se assim um vetor de fomento à indústria nacional de hardware. Paralelamente, o Brasil deve considerar a adoção de padrões abertos e interoperáveis nos contratos públicos de nuvem, condicionando a participação de Big Techs estrangeiras à auditabilidade do código (especialmente do núcleo proprietário da plataforma) e à adoção de arquiteturas que permitam migração futura sem *lock-in*. Com políticas industriais robustas que integrem regulação, compras governamentais e estímulo à produção local, o Brasil pode transformar sua vulnerabilidade atual em ativo de soberania

Com base nos achados desta pesquisa, as principais contribuições deste trabalho se materializam em proposições para um modelo mais robusto e soberano de adoção de nuvem pelo Estado. Primeiramente, recomenda-se a instrumentalização da MRC, a Matriz de Requisitos Contratuais desenvolvida nesta pesquisa poderia ser utilizada como um checklist obrigatório e dinâmico por todos os órgãos da Administração Pública Federal, sendo disponibilizada pela Secretaria de Governo Digital juntamente aos demais materiais de apoio à contratação de soluções de tecnologia [66]. A institucionalização de cláusulas anti-lock-in, é essencial e também deve ser considerada, pois a constatação de contratos de longa duração (com vigência decenal), demonstra a urgência de se exigir, como cláusula obrigatória em toda contratação de nuvem de grande porte, a previsão explícita dos custos de saída (egress) e a garantia de portabilidade em formatos abertos e estruturados (ex: OVF, CSV, JSON), preferencialmente com a fixação de "custo zero" para a transferência dos dados ao final do contrato. Tal exigência deveria ser objeto de normativo conjunto do MGI e do GSI, dada sua relevância estratégica para a soberania digital. Outra medida essencial está relacionada à operacionalização do RIPD nas Contratações. A persistente ausência do RIPD nos contratos, inclusive nos mais recentes, indica a necessidade de uma diretriz específica da ANPD ou do MGI que torne obrigatória, para contratações de médio e alto risco, a apresentação, pelo provedor, das informações técnicas necessárias à elaboração do RIPD pelo controlador, ou a apresentação de seu próprio RIPD para validação prévia à contratação. Esta medida é essencial para que a Administração cumpra seu dever de transparência e gestão de riscos. Em relação aos aspectos técnicos, torna-se imprescindível o fomento à autonomia tecnológica. A estratégia de nuvem deve ser acompanhada por uma política industrial e de inovação que condicione as parcerias com Big Techs à transferência efetiva de tecnologia, ao

investimento em pesquisa e desenvolvimento no Brasil e à criação de incentivos para o desenvolvimento de um ecossistema nacional de software livre e hardware aberto.

A pesquisa também evidencia que para fortalecimento da governança, qualquer que seja a estratégia adotada para nuvens no governo, é imperativo investir na capacitação contínua dos quadros técnicos e jurídicos dos órgãos públicos e das estatais (Serpro, Dataprev) para que possam exercer plenamente seu papel de controladores. Isso inclui dominar ferramentas de auditoria contínua, compreender os modelos de responsabilidade compartilhada e utilizar proativamente o RIPD como instrumento de gestão de riscos. Analisando o cenário num contexto mais estratégico, é relevante ponderar sobre aspectos relacionados à articulação internacional e regulatória. O Brasil poderia atuar diplomaticamente para utilizar fóruns, como no âmbito dos BRICS, ou até mesmo na América Latina, para instigar o debate sobre a promoção de um modelo de governança de dados alternativo ao domínio das Big Techs. Em âmbito nacional, é importante que a ANPD e o GSI atuem de forma coordenada para garantir que a regulação de transferências internacionais e o tratamento de dados classificados sejam efetivamente auditáveis e capazes de proteger o interesse público. A soberania de dados torna-se assim não apenas uma questão técnica, mas política, econômica e cultural, essencial para que o Brasil possa desenvolver tecnologias para a demanda nacional, reduzindo a subordinação digital e garantindo maior autonomia no cenário global. Sem uma regulação forte e uma visão estratégica de longo prazo, o Brasil corre o risco de submeter sua transformação digital a interesses estrangeiros, comprometendo sua soberania e autonomia tecnológica.

Em suma, a trajetória atual da Administração Pública Federal, embora tenha dado passos importantes, ainda não provê os instrumentos necessários para sustentar efetivamente a soberania de dados e consequentemente a conformidade com a LGPD de uma forma mais robusta. A verdadeira proteção de dados sigilosos e a viabilização da privacidade no setor público exigirão, para além da localização física, o desenvolvimento de capacidades tecnológicas próprias, marcos regulatórios robustos contra ingerências externas e, sobretudo, uma clara definição sobre qual modelo de soberania digital o país pretende construir. O desafio que se coloca não é meramente técnico ou contratual, mas essencialmente político e estratégico, é preciso definir se o Brasil será um mero consumidor de tecnologia estrangeira ou se disporá a construir as bases de uma autonomia digital duradoura, que coloque a tecnologia a serviço do desenvolvimento nacional e da proteção dos direitos fundamentais de seus cidadãos. Do mesmo modo, a efetividade da LGPD como ferramenta de soberania está condicionada à sua articulação sinérgica com políticas de Estado que promovam a infraestrutura tecnológica nacional, fomentem a inovação e regulem assertivamente a atuação de atores transnacionais, convertendo o arcabouço protetivo individual em um instrumento efetivo de autodeterminação informacional coletiva.

### *A. Trabalhos Futuros*

Os achados desta pesquisa abrem múltiplas agendas de investigação para o aprofundamento da soberania digital e da conformidade com a LGPD no setor público. Em primeiro lugar, recomenda-se a ampliação do escopo da análise documental para contratos de outros entes federativos (estados, municípios) e de outros poderes (Judiciário, Legislativo), de modo a verificar se as lacunas aqui identificadas, especialmente a ausência de custos de saída e a subutilização do RIPD, se reproduzem ou assumem novas configurações. Em segundo lugar, seria profícuo um estudo de caso longitudinal que acompanhe, ao longo de todo o ciclo de vida de um contrato de Nuvem de Governo (ex: MGI 65/2025), a efetividade real das cláusulas de soberania e segurança, incluindo a realização de auditorias independentes e a verificação da capacidade operacional das estatais (Serpro, Dataprev) para exercer o controle determinante sobre o núcleo proprietário das Big Techs. Em terceiro lugar, a recente publicação da IN GSI/PR nº 8/2025 (dados classificados) e da Resolução CD/ANPD nº 19/2024 (transferências internacionais) demanda estudos específicos sobre sua internalização nos contratos e sua eficácia na mitigação dos riscos de ingerência extraterritorial. Por fim, do ponto de vista das políticas públicas, sugere-se uma pesquisa de prospecção tecnológica e econômica sobre a viabilidade de se condicionar as parcerias com Big Techs à transferência efetiva de tecnologia e ao desenvolvimento de um ecossistema nacional de software livre e hardware aberto, articulando a estratégia de nuvem com a cadeia de valor das terras raras e a Política Nacional de Data Centers recentemente lançada.

Agradecimentos

À minha esposa, pelo apoio incondicional, paciência e compreensão durante toda a jornada de pesquisa e escrita. À Universidade de Brasília (UnB), em especial ao Programa de Pós-Graduação Profissional em Engenharia Elétrica (PPEE), pelo ambiente acadêmico de excelência e pelas oportunidades de aprendizado e desenvolvimento profissional. Ao Ministério da Gestão e da Inovação em Serviços Públicos (MGI), pela parceria institucional que viabilizou esta especialização, permitindo a articulação entre a prática da administração pública federal e o rigor acadêmico. Aos professores e colegas de turma, pelas discussões enriquecedoras e pelo compartilhamento de experiências e, em especial ao meu orientador, cujas considerações qualificaram sobremaneira este trabalho.

REFERÊNCIAS


[1] ZUBOFF, Shoshana. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs, 2019. Disponível em: https://www.proquest.com/openview/c20240e59a5f76707aa2abd1faa4fe5d/1?pq-origsite=gscholar&cbl=396354. Acesso em 28 Jan. 2026.

[2] SILVA, Fabiano Couto Corrêa da; PIRES, Thalia da Silva; WENDT, Lucas George. Do colonialismo histórico ao colonialismo de dados: reflexões sobre a relação entre Big Data e o sujeito. LOGEION: Filosofia da Informação, Rio de Janeiro, v. 10, n. 1, p. 75–90, ago. 2023/jan. 2024. DOI: 10.21728/logeion.2023v10n1.p75-90.

[3] PENTEADO, Cláudio; PELLEGRINI, Jerônimo; SILVEIRA, SA da. Plataformização, inteligência artificial e soberania de dados: tecnologia no Brasil 2020-2030. São Paulo: Ação Educativa, 2023. Disponível em: https://acaoeducativa.org.br/wp-content/uploads/2024/01/tecnologia_no_brasil_2020_2030.pdf. Acesso em: 16/01/2026.

[4] MASSUCHIN, Michele Goulart; TAVARES, Camilla Quesada; COMEL, Naiza. SOBERANIA DIGITAL E INFORMACIONAL: desafios da gestão de tecnologias, da comunicação pública e os reflexos para a cidadania. In: COMPÓS. 2025.

[5] VAN HAMOND, Johannes Maria. Evaluating Sovereignty Claims of US Hyperscalers in Europe: A Comprehensive Audit of Legal, Technical, and Governance Controls for Digital Autonomy. LawArXiv, 27 jul. 2025. Disponível em: https://osf.io/preprints/lawarxiv/953fb_v1. Acesso em: 13 abr. 2026.

[6] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018.

[7] MENDES, L. S.; MARINHO, R. P. A proteção de dados pessoais no Brasil e a LGPD: um panorama inicial. Revista de Internet, Direito e Política, [S. l.], n. 30, p. 1-15, 2020.

[8] DONEDA, D.; ALMEIDA, V. A. F. Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados. Revista de Direito Administrativo, Rio de Janeiro, v. 276, p. 27-57, maio/ago. 2019.

[9] MECABÔ, Alex. Proteção de dados pessoais: a função e os limites do consentimento, de Bruno Bioni. Revista de Direito Civil Contemporâneo, v. 28, p. 427-443, 2021.

[10] OLIVEIRA, M. V. S. et al. Governança de dados pessoais no setor público: perspectivas para a implementação da LGPD. Revista do Serviço Público, Brasília, v. 71, n. 4, p. 791-822, out./dez. 2020. ISSN 2357-8017.

[11] National Institute of Standards and Technology, NIST, “The NIST Definition of Cloud Computing,” Set. 2011. [Online]. Disponível em: https://doi.org/10.6028/nist.sp.800-145. Acesso em 15 jan. 2026.

[12] GARTNER. Information Technology Glossary: Cloud Computing. [S. l.], 2023. Disponível em: https://www.gartner.com/en/information-technology/glossary/cloud-computing. Acesso em: 15 jan. 2026.

[13] European Union Agency for Cybersecurity. Cloud Computing: Benefits, Risks and Recommendations for Information Security. Heraklion: ENISA, 2009. Disponível em: https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment/at_download/fullReport. Acesso em: 15 jan. 2026.

[14] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 17788: Tecnologia da informação — Computação em nuvem — Visão geral e vocabulário. Rio de Janeiro: ABNT, 2014.

[15] GARCÍA ZABALLOS, Antonio et al. Contratação pública de serviços de computação em nuvem: melhores práticas para sua implementação na América Latina e no Caribe. Washington, D.C.: Banco Interamericano de Desenvolvimento, 2020. 96 p. (Monografia do BID, 807). Disponível em: https://publications.iadb.org/publications/portuguese/document/Contratacao-publica-de-servicos-de-computacao-em-nuvem-Melhores-praticas-para-sua-implementacao-na-America-Latina-e-no-Caribe.pdf. Acesso em: 27 jan. 2026.

[16] BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Secretaria de Governo Digital. Estratégia de Governança e Transformação Digital para o Sistema de Administração dos Recursos de Tecnologia da Informação e Comunicação do Poder Executivo Federal (EGTIC). Brasília, [s.d.]. Disponível em: https://www.gov.br/governodigital/pt-br/estrategia-de-governanca-digital/EGTIC.pdf. Acesso em: 25 jan. 2026.

[17] BRASIL. Histórico da Estratégia de Governo Digital. Brasília, DF: [s. n.], 2025. Disponível em: https://www.gov.br/governodigital/pt-br/estrategia-de-governanca-digital/historico. Acesso em: 3 fev. 2026.

[18] BRASIL. Decreto nº 10.332, de 28 de abril de 2020. Institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, 29 abr. 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10332.htm Acesso em: 02 jan. 2026.

[19] BRASIL. Secretaria de Governo Digital. Um Governo Transparente, Aberto e Participativo. Brasília, 2023. Disponível em: https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/EFGD/transparente-aberto-participativo. Acesso em: 12 fev. 2026.

[20] BRASIL. Instrução Normativa SGD/ME n. 94, de 23 de dezembro de 2022. Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação – TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação – SISP. Diário Oficial da União: seção 1, Brasília, DF, p. 114, 29 dez. 2022.

[21] MEDEIROS, Marcos Fernando Machado de; NETO, Manoel Veras Sousa. Uso da computação em nuvem no setor público: um estudo de caso com gestores de TI do estado do Rio Grande do Norte e do Governo Federal. Revista Gestão & Tecnologia, Pedro Leopoldo, v. 16, n. 1, p. 135-156, 2016. Disponível em: https://doi.org/10.20397/2177-6652/2016.v16i1.790. Acesso em: 27 jan. 2026.

[22] AGÊNCIA DA UNIÃO EUROPEIA PARA A CIBERSEGURANÇA (ENISA). ENISA threat landscape 2023: the rise of hybrid warfare: the cloud threat landscape (Capítulo 4). [S. l.], out. 2023. Disponível em: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023. Acesso em: 21 jan 2026.
[23] CLOUD SECURITY ALLIANCE. Security Guidance for Critical Areas of Focus in Cloud Computing v5. 2024. Disponível em: https://cloudsecurityalliance.org/artifacts/security-guidance-v5/. Acesso em: 17 jan. 2026.
[24] CLOUD SECURITY ALLIANCE. Cloud Controls Matrix (CCM): security assurance and risk management for cloud 29]computing. v4. 2021. Disponível em: https://cloudsecurityalliance.org/research/cloud-controls-matrix/. Acesso em: 19 jan. 2026.
[25] National Institute of Standards and Technology, NIST, “Guidelines on Security and Privacy in Public Cloud Computing”, Set. 2011. Disponível em: https://doi.org/10.6028/NIST.SP.800-144. Acesso em 15 Jan. 2026.
[26] AHMADI, Sina. Systematic literature review on cloud computing security: threats and mitigation strategies. Journal of Information Security, v. 15, p. 148–167, 2024. DOI: 10.4236/jis.2024.152010. Disponível em: https://doi.org/10.4236/jis.2024.152010. Acesso em: 20 jan. 2026.
[27] BASIT, Abdul; KHAN, Muhammad Asif; HUSSAIN, Shahzad; et al. Security threats on cloud computing vulnerabilities. International Journal of Advanced Computer Science and Applications, v. 15, n. 3, p. 1–12, 2024. Disponível em: https://thesai.org/Publications/ViewPaper?Volume=15&Issue=3&Code=IJACSA&SerialNo=1. Acesso em: 20 jan. 2026.
[28] NUNES, Rafael R. P. dos S. et al. Benefícios e Riscos do Uso da Computação em Nuvem no Setor Público: uma análise baseada em artigos disponibilizados em bases de dados acadêmicas de 2017 a 2021. 2022. Disponível em: https://www.researchgate.net/profile/Rafael-Nunes-4/publication/362918198_Beneficios_e_Riscos_do_Uso_da_Computacao_em_Nuvem_no_Setor_Publico_uma_analise_baseada_em_artigos_disponibilizados_em_bases_dados_academicas_de_2017_a_2021/links/63076e7bacd814437fd6c16d/Beneficios-e-Riscos-do-Uso-da-Computacao-em-Nuvem-no-Setor-Publico-uma-analise-baseada-em-artigos-disponibilizados-em-bases-dados-academicas-de-2017-a-2021.pdf. Acesso em: 26 jan. 2026.
[29] CLOUD SECURITY ALLIANCE. Top threats to cloud computing 2024. [S.l.]: Cloud Security Alliance, 2024. Disponível em: https://cloudsecurityalliance.org. Acesso em: 20 jan. 2026.
[30] OWASP FOUNDATION. OWASP Top Ten. [S. l.], 2025. Disponível em: https://owasp.org/www-project-top-ten/. Acesso em: 23 jan. 2026.
[31] MICROSOFT. Microsoft Digital Defense Report 2025. Redmond, WA: Microsoft, 2025. Disponível em: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf. Acesso em: 24 jan. 2026.
[32] GOOGLE CLOUD. Office of the CISO. Cloud Threat Horizons Report: H2 2025. [S. l.], 2025. Disponível em: https://services.google.com/fh/files/misc/cloud_threat_horizons_report_h22025.pdf. Acesso em: 24 jan. 2026.
[33] AMAZON WEB SERVICES. Brazil General Data Protection Law (LGPD) Workbook. 2022. Disponível em: https://d1.awsstatic.com/whitepapers/compliance/Brazil_General_Data_Protection_Law_Workbook_English_2022.pdf. Acesso em: 03 fev. 2023.
[34] AMAZON WEB SERVICES. LGPD Compliance on AWS. 2022. Disponível em: https://d1.awsstatic.com/whitepapers/compliance/LGPD_Compliance_on_AWS.pdf. Acesso em: 03 fev. 2023.
[35] GOOGLE. Google Cloud & Lei Geral de Proteção de Dados (LGPD) - Guia de Referência Rápida. 2020. Disponível em: https://services.google.com/fh/files/misc/googlecloud_lgpd_quick_reference_guide_dec_2020.pdf. Acesso em: 3 fev. 2026.
[36] HUAWEI. HUAWEI CLOUD Compliance Instruction with Brazil LGPD. 2025. Disponível em: https://res-static.hc-cdn.cn/cloudbu-site/intl/en-us/TrustCenter/WhitePaper/privacy/Brazil_LGPD_Compliance_intl_en.pdf. Acesso em: 4 fev. 2026.
[37] SILVA, Ergon Cugler de Moraes et al. Entre licenças bilionárias e nuvens internacionais: um mapeamento sistemático de contratos do setor público brasileiro com fornecedores internacionais de tecnologias. InterAção, Santa Maria, v. 16, n. 4, p. e93697, 30 set. 2025. Disponível em: https://doi.org/10.5902/2357797593697. Acesso em: 27 jan. 2026.
[38] GINGLASS, Mário Roberto. Soberania e uso de tecnologias emergentes e de serviços de computação em nuvem por empresas públicas federais no Brasil. 2024.Disponível em: https://repositorio.esg.br/handle/123456789/1973. Acesso em: 3 fev. 2026.
[39] PINHEIRO JUNIOR, Luiz Pereira; CUNHA, Maria Alexandra Viegas Cortez da. CloudGov: aspectos organizacionais, institucionais e contextuais da computação em nuvem no governo. In: ENCONTRO DA ANPAD, 45., 2021, On-line. Anais [...]. On-line: ANPAD, 2021. p. 1-17.
[40] REYES, CRISTINA; MENDOZA, CLARISSE. Exploring the Impact of Shared Responsibility Models on Cloud Security Posture and Vulnerability Management. Quarterly Journal of Emerging Technologies and Innovations, v. 8, n. 1, p. 1-10, 2023.
[41] ORACLE; KPMG. Demystifying the Cloud: Shared Responsibility Security Model. Oracle and KPMG Cloud Threat Report 2020 series, Volume 2. 2020. Disponível em: https://www.oracle.com/a/ocom/docs/cloud/oracle-ctr-2020-shared-responsibility.pdf. Acesso em: 22 jan. 2026.
[42] GOOGLE CLOUD. Responsabilidades compartilhadas e destino compartilhado em Google Cloud. Cloud Architecture Center. Última atualização em: 21 ago. 2023. Disponível em: https://docs.cloud.google.com/architecture/framework/security/shared-responsibility-shared-fate?hl=pt-br. Acesso em: 22 jan. 2026.
[43] Azure, “Shared Responsibility in the Cloud,” Microsoft, 29 Set. 2024. [Online]. Available: https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility. Acesso em: 22 jan. 2026.

[44] CIS - CENTER FOR INTERNET SECURITY. Cloud Security and the Shared Responsibility Model. [S. l.]: CIS, 22 fev. 2021. Disponível em: https://www.cisecurity.org/insights/white-papers/cloud-security-and-the-shared-responsibility-model. Acesso , 15em: 5 fev. 2026.
[45] FULEA, Flavia. Toward collaborative and cooperative cybersecurity: a survey on approaches, challenges, and opportunities. 2022. 112 f. Communication Systems Group, Department of Informatics, University of Zurich, Zurich, 2022. Disponível em: https://capuana.ifi.uzh.ch/publications/PDFs/22764__MA_Toward_Collaborative_and_Cooperative_Cybersecurity__A_Survey_on_Approaches__Challenges__and_Opportunities_Final.pdf. Acesso em: 3 fev. 2026.
[46] AWS (Amazon Web Services). AWS Data Processing Addendum. Seattle: Amazon Web Services, [202-?]. Disponível em: https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf. Acesso em: 24 mar. 2026.
[47] GOOGLE. Aditivo sobre Tratamento de Dados do Cloud (clientes). Mountain View: Google, [202-?]. Disponível em: https://services.google.com/fh/files/misc/pt-br-cloud-data-processing-addendum-customers.pdf. Acesso em: 24 mar. 2026.
[48] THOTA, Ravi Chandra. Cloud-Native DevSecOps: Integrating Security Automation into CI/CD Pipelines. International Journal of Innovative Research and Creative Technology, v. 10, n. 6, p. 1-19, 2024. DOI: 10.5281/zenodo.15036934. Disponível em: https://doi.org/10.5281/zenodo.15036934 Acesso em: 6 fev. 2026.
[49] SIMHADRI, Sindhu. From shared responsibility to shared fate: redefining cloud security paradigms in multi-cloud environments. Cloud and Future Security, [S. l.], v. 377, 2025. DOI: https://doi.org/10.52710/cfs.850. Disponível em: https://doi.org/10.52710/cfs.850. Acesso em: 6 fev. 2026.
[50] BRASIL. Tribunal de Contas da União. Acórdão nº 1739/2015 – Plenário. Relator: Ministro Benjamin Zymler. Processo TC 025.994/2014-0. Diário Eletrônico da Justiça Federal, Brasília, DF, 15 jul. 2015.
[51] BRASIL. Instrução Normativa nº 1, de 27 de maio de 2020. Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal. Diário Oficial da União: seção 1, Brasília, ano 158, n. 101-A, p. 2, 28 mai. 2020. Edição extra. Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-1-de-27-de-maio-de-2020-258915215.. Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-5-de-30-de-agosto-de-2021-341649684. Acesso em: 11 fev. 2026.
[52] BRASIL. Instrução Normativa nº 5, de 30 de agosto de 2021. Dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal. Diário Oficial da União, Brasília, DF, ed. 165, seção 1, p. 2, 31 ago. 2021.
[53] BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Secretaria de Governo Digital. Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023. Dispõe sobre o modelo de contratação de software e serviços em nuvem no âmbito da administração pública federal. Brasília, DF, 2023. Disponível em: https://www.gov.br/governodigital/pt-br/contratacoes-de-tic/legislacao/modelo-de-contratacao-de-software-e-servicos-em-nuvem/vigentes/portaria-sgd-mgi-no-5-950-de-26-de-outubro-de-2023. Acesso em: 26 mar. 2026.
[54] BRASIL. Gabinete de Segurança Institucional da Presidência da República. Instrução Normativa GSI/PR nº 8, de 6 de outubro de 2025. Dispõe sobre os requisitos mínimos de segurança da informação para tratamento de informação classificada em computação em nuvem. Diário Oficial da União: seção 1, Brasília, DF, ano 162, n. 191, p. 1, 7 out. 2025.
[55] DATAPREV. Brasil consolida a Nuvem de Governo como passo para a independência e a proteção de dados. Rio de Janeiro, 8 set. 2025. Disponível em: https://portal3.dataprev.gov.br/noticias/brasil-consolida-nuvem-de-governo-como-passo-para-independencia-e-protecao-de-dados. Acesso em: 2 mar. 2026.
[56] SERPRO. Soberania, segurança e solidez: Serpro detalha a Nuvem de Governo em encontro com gestores federais de TI. Brasília, 22 jul. 2025. Disponível em: https://www.serpro.gov.br/menu/noticias/noticias-2025/serpro-detalha-nuvem-de-governo-ao-sisp. Acesso em: 2 mar. 2026.
[57] BNAMERICAS. Spotlight: Brazil’s government cloud project. Santiago, 7 out. 2024. Disponível em: https://www.bnamericas.com/en/news/spotlight-brazils-government-cloud-project. Acesso em: 2 mar. 2026.
[58] MORAES, Gabriel Boscardim. Empresas públicas para a soberania nacional: o caso do Serpro com as Big Techs e outras possibilidades. Îandé: Ciências e Humanidades, São Bernardo do Campo (SP), v. 8, n. 1, p. 65–80, 2024.DOI: 10.36942/iande.v8i1.985.
[59] BAUR, Andreas. European Dreams of the Cloud: Imagining Innovation and Political Control. Geopolitics, v. 29, n. 2, p. 417-434, 2024. DOI: 10.1080/14650045.2022.2151902. Disponível em: https://www.tandfonline.com/doi/full/10.1080/14650045.2022.2151902. Acesso em: 27 mar. 2026.
[60] VAN HAMOND, Johannes Maria. Evaluating sovereignty claims of US hyperscalers in Europe: a comprehensive audit of legal, technical, and governance controls for digital autonomy. LawArchive, Center for Open Science, 27 jul. 2025. DOI: 10.31219/osf.io/953fb_v1. Disponível em: https://econpapers.repec.org/paper/osflawarc/953fb_5fv1.htm. Acesso em: 27 mar. 2026.
[61] BLANCATO, Filippo Gualtiero. The cloud sovereignty nexus: How the European Union seeks to reverse strategic dependencies in its digital ecosystem. Policy & Internet, v. 15, n. 4, p. 456-472, 2023. DOI: 10.1002/poi3.358. Disponível em: https://onlinelibrary.wiley.com/doi/full/10.1002/poi3.358. Acesso em: 27 mar. 2026.
[62] ADLER-NISSEN, Rebecca; EGGELING, Kristin Anabel. The discursive struggle for digital sovereignty: security, economy, rights and the cloud project Gaia-X. Journal of Common Market Studies, Oxford, v. 62, n. 4, p. 993–1011, jul. 2024. DOI: 10.1111/jcms.13594. Disponível em: https://onlinelibrary.wiley.com/doi/10.1111/jcms.13594. Acesso em: 3 mar. 2026.

[63] MARQUES, Rodrigo Moreno; DE OLIVEIRA, Vinícius Sousa. O setor de data centers no Brasil: um retrato da falta de soberania tecnológica do país. Liinc em Revista, v. 21, n. 1, p. e7539, 2025.
[64] AGÊNCIA DA UNIÃO EUROPEIA PARA A CIBERSEGURANÇA (ENISA). Cloud Cybersecurity Market Analysis. Heraklion: ENISA, 2023. Disponível em: https://www.enisa.europa.eu/sites/default/files/publications/Cloud%20Cybersecurity%20Market%20Analysis.pdf. Acesso em: 19 jan. 2026.
[65] BRASIL. Autoridade Nacional de Proteção de Dados. Conselho Diretor. Resolução CD/ANPD nº 19, de 23 de agosto de 2024. Aprova o Regulamento de Transferência Internacional de Dados e o conteúdo das cláusulas-padrão contratuais. Diário Oficial da União: seção 1, Brasília, DF, ano 163, p. 123, 23 ago. 2024. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-19-de-23-de-agosto-de-2024-580095396. Acesso em: 01/02/2026.
[66] BRASIL. Secretaria de Governo Digital. Ministério da Gestão e da Inovação em Serviços Públicos. Templates de artefatos para contratação e lista de verificação. Brasília, 2026. Disponível em: https://www.gov.br/governodigital/pt-br/contratacoes-de-tic/orientacoes-e-apoio-especializado/templates-de-artefatos-para-contratacao-e-lista-de-verificacao. Acesso em: 27 mar. 2026.
[67] CAVALCANTI, Leonardo. O projeto do governo para trazer os dados federais "de volta para casa". NeoFeed, 10 set. 2025. Disponível em: https://neofeed.com.br/poder/o-projeto-do-governo-para-trazer-os-dados-federais-de-volta-para-casa/. Acesso em: 26 maio 2026
[68] GEOCRACIA. Sob pressão geopolítica, Brasil acelera corrida por nuvens locais e soberania dos dados. Geocracia, 4 dez. 2025. Disponível em: https://geocracia.com/sob-pressao-geopolitica-brasil-acelera-corrida-por-nuvens-locais-e-soberania-dos-dados/. Acesso em: 26 maio 2026