Análise comparativa dos requisitos de segurança da informação entre Brasil, França, União Europeia e Five Eyes para o tratamento de informações classificadas em nuvem

Diego Braga Serpa[1] **, Robson de Oliveira Albuquerque**[2]

[1]Universidade de Brasília – UnB
Pós-Graduação Lato Sensu em Privacidade e Segurança da Informação
serpa@tutanota.de

[2]Universidade de Brasília – UnB
Programa de Pós-Graduação Profissional em Engenharia Elétrica (PPEE)
robson@redes.unb.br

Resumo. *A Instrução Normativa GSI/PR n.º 8, de 6 de outubro de 2025 (IN 8/2025), disciplinou pela primeira vez, no Brasil, o tratamento de informações classificadas em computação em nuvem pelo Poder Executivo federal. Por ser marco recente e sem precedente doméstico, seus requisitos ainda não haviam sido objeto de avaliação acadêmica sistemática. Este artigo compara o quadro brasileiro com referenciais de França, União Europeia, Estados Unidos da América, Reino Unido, Austrália, Nova Zelândia e Canadá. A análise utiliza matriz comparativa com nove critérios, distribuídos em grupo estrutural (escopo, habilitação, responsabilidade compartilhada, soberania jurisdicional e credenciamento de pessoas) e técnico-operacional (gerenciamento de chaves, localização de dados, auditoria independente e cadeia de suprimentos de TIC). A pesquisa combina análise documental sistemática, direito comparado funcional e pedidos de acesso à informação dirigidos a órgãos do Poder Executivo federal. Os resultados confirmam lacunas críticas: ausência de previsão sobre cadeia de suprimentos; proteção jurisdicional apenas indireta diante de legislações extraterritoriais, como o CLOUD Act; especificação insuficiente para gerenciamento de chaves e criptografia de Estado; e auditoria limitada ao padrão SOC 2 e à autoauditoria pelo órgão contratante. Conclui-se que o quadro brasileiro converge no desenho estrutural, mas se distancia dos requisitos de soberania operacional dos referenciais comparados. Como contribuição, propõem-se seis recomendações de aprimoramento normativo ancoradas em modelos internacionais funcionalmente equivalentes.*

Palavras-chave: segurança da informação; computação em nuvem; informações classificadas; IN GSI/PR n.º 8/2025; análise comparativa; soberania digital.

Abstract. *Normative Instruction No. 8, issued on October 6, 2025, by Brazil's Institutional Security Cabinet of the Presidency (GSI/PR) (IN 8/2025), was the first Brazilian regulation to govern the processing of classified information in cloud computing by the federal Executive branch. As a recent instrument without domestic precedent, its requirements had not yet been systematically assessed. This article compares the Brazilian framework with reference frameworks from France, the European Union, the United States, the United Kingdom, Australia, New Zealand, and Canada. The analysis uses a comparative matrix structured around nine criteria, grouped into a structural set (classification scope, provider authorization, shared responsibility, jurisdictional sovereignty, and personnel security clearance) and a technical-operational set (cryptographic key management, data localization, independent auditing, and ICT supply*

chain security). The research combines systematic document analysis, functional comparative law, and freedom-of-information requests filed with federal Executive bodies. The findings confirm critical gaps: absence of supply-chain security provisions; only indirect jurisdictional protection against extraterritorial legislation, such as the U.S. CLOUD Act; insufficient specification of key management and government-developed cryptographic algorithms; and weak auditing, limited to the SOC 2 standard and self-auditing by the contracting body. The article concludes that the Brazilian framework converges with the comparators in structural design, but falls short of their operational sovereignty requirements. As a contribution, it proposes six recommendations for normative improvement, each anchored in functionally equivalent international models.

Keywords: information security; cloud computing; classified information; IN GSI/PR No. 8/2025; comparative analysis; digital sovereignty.

1. Introdução

A transformação digital do setor público deslocou a computação em nuvem da condição de alternativa de infraestrutura para a de escolha preferencial da administração pública, impulsionada por doutrinas como a *Cloud First* (Brasil, 2022). Essa trajetória é frequentemente interpretada à luz do paradigma da governança da Era Digital (*digital-era governance*, DEG), que identifica a tecnologia da informação como determinante da capacidade estatal e adverte, desde sua formulação original, para a dependência dos governos em relação a grandes integradores e fornecedores de tecnologia (Dunleavy *et al.*, 2006; Margetts; Dunleavy, 2013). No setor público, a adoção de nuvem promete ganhos de escala, elasticidade e custo (Liang *et al.*, 2019), mas também intensifica problemas clássicos de segurança da informação e dependência de fornecedor, além de recolocar, em novo patamar, a questão do controle jurisdicional sobre os dados (Irion, 2012; Paquette; Jaeger; Wilson, 2010).

Esses problemas assumem dimensão de segurança nacional quando envolvem informações classificadas em grau de sigilo. A possibilidade de acesso a dados governamentais por autoridades estrangeiras, viabilizada por legislações como o *Clarifying Lawful Overseas Use of Data Act* (CLOUD Act), somada à concentração do mercado global de nuvem em poucos provedores, converte a escolha de infraestrutura em matéria de soberania (EUA, 2018; Irion, 2012; Roguski, 2025). Por essa razão, a soberania digital tornou-se eixo explícito de políticas públicas em diferentes jurisdições (Pohle; Thiel, 2020; Roberts *et al.*, 2021), embora seu conceito permaneça objeto de disputa e de uso retórico (Ruohonen, 2021).

No Brasil, esse movimento culminou na publicação da Instrução Normativa do Gabinete de Segurança Institucional da Presidência da República (GSI/PR) n.º 8, de 6 de outubro de 2025 (IN 8/2025), primeira norma a disciplinar especificamente o tratamento de informações classificadas em computação em nuvem no âmbito do Poder Executivo federal. O ato normativo articula o regime de credenciamento de segurança do Decreto n.º 7.845/2012 com requisitos técnicos de segurança da informação e insere-se no contexto da terceira geração da Política Nacional de Segurança da Informação (PNSI),[1] instituída pelo Decreto n.º 12.572/2025 (Brasil, 2025b, 2012b, 2025d). Por se tratar de marco recente e sem precedente brasileiro direto, a IN 8/2025 ainda não foi objeto de avaliação acadêmica sistemática quanto à adequação de seus requisitos frente aos referenciais de outros Estados nacionais ou jurisdições.

[1] Conforme sustentam os agentes públicos envolvidos na edição da norma (Molina; Pinto; Portella, 2025).

A IN 8/2025 enfrenta um desafio de adequação: transpõe ao ambiente de nuvem um regime de credenciamento concebido em torno da custódia de informação classificada em instalações físicas determinadas, e o faz sem precedente doméstico que sirva de parâmetro. Disso decorre que não se sabe se os requisitos por ela fixados são adequados, excessivos ou deficientes frente ao que jurisdições com regimes consolidados estabelecem, incerteza com consequências tanto de segurança nacional quanto de viabilidade do próprio modelo.

Diante desse cenário, formula-se o seguinte problema: *em comparação com referenciais de outras jurisdições selecionadas, que convergências, divergências e lacunas podem ser identificadas nos requisitos de segurança da informação estabelecidos pelo quadro normativo brasileiro, em especial pela IN 8/2025, para o tratamento de informações classificadas em computação em nuvem pelo Poder Executivo federal?*

A investigação proposta restringe-se ao plano normativo, isto é, ao conteúdo dos requisitos tal como positivados, sem abranger as condições concretas de implementação pelos órgãos e entidades do Poder Executivo federal, que podem constituir objeto de trabalhos futuros. A análise incide, portanto, sobre o que as normas preveem, e não sobre o grau de execução alcançado por cada jurisdição. Não obstante, a arquitetura normativa e sua completude influenciam as condições de implementação (Haug; Dan; Mergel, 2024). Para contextualizar esse ponto, a investigação utiliza evidências obtidas por pedidos de acesso à informação e achados de fiscalização do Tribunal de Contas da União (TCU).

O objetivo geral é comparar os requisitos de segurança da informação estabelecidos pelo quadro normativo brasileiro para o tratamento de informações classificadas em computação em nuvem pelo Poder Executivo federal com os requisitos correspondentes previstos em referenciais de outras jurisdições selecionadas, identificando convergências, divergências e lacunas.

São objetivos específicos:

a) sistematizar os requisitos de segurança da informação presentes no quadro normativo brasileiro aplicável ao tratamento de informações classificadas em computação em nuvem, compreendendo a legislação de acesso à informação, os decretos regulamentadores e os atos normativos inferiores a decreto;
b) selecionar e sistematizar referenciais de outras jurisdições aplicáveis ao tratamento de informações classificadas em nuvem, segundo critérios de elegibilidade e de composição definidos na metodologia;
c) construir matriz comparativa estruturada pelos critérios identificados; e
d) formular recomendações de aprimoramento normativo para os requisitos do quadro brasileiro, com base nas lacunas identificadas na análise comparativa.

A pesquisa testa a seguinte hipótese: o quadro normativo brasileiro apresenta lacunas em requisitos críticos de segurança da informação identificados na matriz comparativa. A hipótese é testada pela análise comparativa entre o quadro normativo brasileiro e os outros referenciais selecionados.

Além desta introdução, o artigo apresenta o referencial teórico (Seção 2); a revisão de literatura (Seção 3), que situa o estado da arte e a lacuna a preencher; a metodologia (Seção 4); os resultados (Seção 5), com a sistematização do quadro brasileiro e a matriz comparativa; a discussão (Seção 6), que confronta a hipótese e formula recomendações de aprimoramento normativo; e a conclusão (Seção 7).

2. Referencial teórico

Esta seção reúne as bases conceituais que sustentam a análise comparativa. Situa-se, inicialmente, a adoção de nuvem no setor público como fenômeno institucional, à luz do paradigma da

governança da Era Digital. Adota-se, na sequência, a distinção entre regras e princípios como ferramenta para interpretar os requisitos de segurança da informação. Delimita-se, então, a acepção de soberania digital empregada no trabalho, a taxonomia de computação em nuvem de referência e, por fim, a demarcação entre segurança da informação, segurança cibernética e informação classificada, categorias que informam os critérios da matriz comparativa apresentada adiante.

2.1. Governo digital e adoção de nuvem no setor público

O paradigma da governança da Era Digital sustenta que a tecnologia da informação deixou de ser instrumento acessório para tornar-se determinante estrutural da capacidade do Estado, sucedendo o *New Public Management* como quadro dominante de modernização administrativa (Dunleavy *et al.*, 2006). Sua segunda formulação incorpora a digitalização plena, a reintegração de serviços e o dado como ativo central, antecipando o ambiente de nuvem e *big data* em que operam hoje as administrações públicas (Margetts; Dunleavy, 2013). Revisões sistemáticas recentes da transformação digital do setor público convergem na constatação de que requisitos legais e o sistema político são indutores de mudança transformativa proporcionalmente mais fortes do que os fatores estritamente tecnológicos (Haug; Dan; Mergel, 2024), o que confere centralidade ao estudo de instrumentos normativos como a IN 8/2025.

A adoção de nuvem no setor público, contudo, não é processo puramente técnico. A literatura identifica desafios persistentes de ordem técnica, organizacional, legal, de privacidade, de segurança e de interoperabilidade (Janssen; Joha, 2011), e demonstra que o governo digital é inovação institucional dependente de regras formais e informais e de mecanismos de *accountability*, e não mera inovação tecnológica (Meijer; Zouridis, 2006; Bannister; Connolly, 2011). Adotada essa perspectiva institucional, a IN 8/2025 e os demais instrumentos normativos são analisados neste trabalho como parte desse desenho, o que fundamenta a abordagem comparada adotada adiante.

2.2. Regras e princípios

Dworkin (2002) e Alexy (2014) distinguem entre regras e princípios: enquanto as primeiras operam como razões definitivas, aplicadas, em regra, por subsunção, os segundos funcionam como mandamentos de otimização, cuja concretização depende de ponderação à luz das circunstâncias do caso concreto. Neste trabalho, a distinção entre regras e princípios é empregada de modo instrumental, como ferramenta para diferenciar enunciados normativos de perfil mais fechado, avaliáveis em termos de conformidade binária (tudo ou nada), de enunciados mais abertos, cuja realização depende de concretização gradual e de juízos de proporcionalidade. Os requisitos de segurança da informação serão interpretados, nessa leitura, como as regras extraíveis dos referenciais selecionados para o tratamento de informações classificadas em nuvem.

2.3. Soberania digital

A soberania digital é um conceito polissêmico. O mapeamento de Pohle e Thiel (2020) distingue seu uso em três categorias de reivindicações de autodeterminação (em favor do Estado, das empresas ou dos indivíduos) e evidencia as tensões internas do conceito, especialmente entre a autoridade estatal e a proteção de direitos individuais e valores democráticos. Análises das políticas europeias mostram uma distância recorrente entre declarações políticas e instrumentos concretos de soberania (Roberts *et al.*, 2021); por sua vez, a crítica epistemológica adverte para o risco de instrumentalização retórica do termo, ao qual são atribuídos ao menos dezesseis significados distintos (Ruohonen, 2021; Christakis, 2020). Em registro mais amplo, a teoria da computação planetária descreve a camada de nuvem como instância que desloca a soberania

territorial westfaliana, sobrepondo uma geografia jurisdicional própria à geografia dos Estados (Bratton, 2015). Sem aderir a essa moldura, este trabalho retém apenas sua principal contribuição analítica, qual seja, a dissociação entre localização física e controle jurisdicional. Para os fins desta pesquisa, adota-se uma acepção operacional e restrita: soberania de dados como a capacidade do Estado de manter controle jurisdicional efetivo sobre informações sob sua guarda, inclusive quando processadas por terceiros (Irion, 2012).

A precariedade do controle jurisdicional sobre dados governamentais está documentada na literatura. A análise de direito internacional demonstra que o regime atual não assegura, por si, proteção efetiva a dados governamentais armazenados no exterior (Roguski, 2025), e que o acesso transfronteiriço a evidências eletrônicas permanece governado por abordagens fragmentárias e por legislações de alcance extraterritorial (Abraha, 2021; Christakis; Terpan, 2021). A concentração da oferta global de nuvem em poucos provedores sujeitos a jurisdições estrangeiras é fator de risco de primeira ordem à continuidade do acesso a capacidades críticas (Baldoni; Di Luna, 2025). No debate brasileiro, essa preocupação tem sido articulada tanto na academia quanto em documentos institucionais (Belli *et al.*, 2026; Brasil, 2026d).

2.4. Computação em nuvem: conceito e modelos

Adota-se a taxonomia do *National Institute of Standards and Technology* (NIST), que define a computação em nuvem por cinco características essenciais (autoatendimento sob demanda, amplo acesso à rede, *pool* de recursos, elasticidade rápida e medição de serviço), três modelos de serviço (IaaS, PaaS e SaaS) e quatro modelos de implantação — pública, privada, comunitária e híbrida (Mell; Grance, 2011). A distinção entre os modelos é, ela própria, uma variável de análise, já que vários referenciais vedam a nuvem pública para informação classificada e a admitem apenas em modelos privado, comunitário ou dedicado.

2.5. Segurança da informação, segurança cibernética e informação classificada

A literatura distingue segurança da informação de segurança cibernética, ainda que os termos sejam, com frequência, empregados como sinônimos. A segurança da informação é centrada na informação e na preservação de sua disponibilidade, integridade, confidencialidade e autenticidade, qualquer que seja o suporte, e abrange dimensões física, organizacional, de pessoas e técnica (ISO/IEC, 2018). A segurança cibernética, por sua vez, é centrada no ciberespaço e nos sistemas que o constituem, alcançando ativos e sujeitos que não são, eles próprios, informação (ABNT, 2025, 2024). Como sustentam Solms e Niekerk (2013), os dois campos se sobrepõem, mas não coincidem: a segurança da informação inclui informação não digital, enquanto a segurança cibernética inclui a proteção de ativos não informacionais e das próprias pessoas contra ameaças oriundas do ciberespaço. A interseção entre os domínios é qualificada como a segurança da informação digital.

No Brasil, essa relação está positivada de modo particular: a segurança cibernética é tratada como *componente* da segurança da informação. A PNSI define a segurança da informação como conceito guarda-chuva, que engloba a segurança cibernética, a defesa cibernética, a segurança física e a proteção de dados organizacionais (Brasil, 2025d). Em paralelo, consolidou-se uma trilha própria de cibersegurança, com a Estratégia Nacional de Segurança Cibernética (Decreto n.º 10.222/2020, substituído pelo Decreto n.º 12.573/2025) e a Política Nacional de Cibersegurança, que instituiu o Comitê Nacional de Cibersegurança (Decreto n.º 11.856/2023) (Brasil, 2020, 2025a, 2023a). Dessa arquitetura resulta uma sobreposição institucional relevante: a segurança da informação permanece sob coordenação do Gabinete de Segurança Institucional da Presidência da República, ao passo que a governança cibernética se desenvolve em instâncias próprias.

O tratamento de informação classificada apoia-se nos atributos clássicos da segurança da informação, formalizados no direito brasileiro desde a Lei de Acesso à Informação (LAI) (Brasil, 2011). A informação classificada distingue-se das demais por seu regime jurídico próprio: graus de sigilo, prazos de restrição e, sobretudo, a exigência de credenciamento de segurança de pessoas e entidades para o seu tratamento (Brasil, 2011, 2012b). Quando esse tratamento migra para a nuvem, somam-se riscos de segurança específicos, já sistematizados na literatura (Paquette; Jaeger; Wilson, 2010) e relacionados, em última análise, à segurança nacional (Abd Al Ghaffar, 2020).

3. Revisão de literatura

Esta seção examina o estado da arte pertinente ao objeto e delimita a lacuna que o artigo se propõe a preencher. A produção existente organiza-se em três eixos: os riscos de segurança da nuvem governamental; o tratamento de informação classificada em nuvem; e a soberania de dados frente ao acesso transfronteiriço, examinados nas subseções seguintes. A eles se segue a constatação da ausência de análise comparada que confronte o regime brasileiro de informação classificada em nuvem, em especial a IN 8/2025, com referenciais de outras jurisdições.

3.1. Riscos de segurança da nuvem governamental

A literatura sobre segurança de nuvem no governo tem como marco o trabalho de Paquette, Jaeger e Wilson (2010), que identifica e categoriza os riscos de segurança associados ao uso governamental de nuvem, distinguindo, entre os riscos tangíveis, as categorias de acesso, disponibilidade, infraestrutura e integridade, além de um amplo conjunto de riscos intangíveis (jurisdição, propriedade da informação e acesso público continuado, entre outros). Estudos empíricos posteriores examinaram os fatores associados à adoção governamental de nuvem, mostrando que a conformidade regulatória e os requisitos legais explicam menos a adoção do que fatores organizacionais como conscientização, segurança operacional e qualidade do acordo de nível de serviço (Ali *et al.*, 2020). Na vertente de valor público, pesquisas sobre a assimilação de nuvem no governo mostram que os benefícios dependem de fatores organizacionais, e não apenas da adoção tecnológica (Liang *et al.*, 2019). A revisão sistemática mais recente sobre segurança e privacidade na adoção de nuvem pelo setor público, conduzida sob protocolo PRISMA, consolida esse acervo e mapeia as categorias de desafios predominantes na literatura de 2019 a 2023 (Ukeje; Gutierrez; Petrova, 2024).

3.2. Tratamento de informação classificada em nuvem

A literatura que trata especificamente de informação classificada em nuvem é mais escassa e, em larga medida, normativa. No Brasil, não foi identificada produção acadêmica específica sobre o tema. O estudo comparado mais próximo do objeto deste artigo analisa os requisitos de segurança para nuvem apenas nos contextos finlandês e europeu (Papaleonidas, 2025). A maior parte do conhecimento disponível encontra-se dispersa nos próprios instrumentos normativos e técnicos de cada jurisdição, tais como referenciais de certificação de provedores, perfis de controle e regras de residência de dados, cuja sistematização comparada constitui parte da contribuição deste trabalho (Seção 5.5 e Apêndice D).

3.3. Soberania de dados e acesso transfronteiriço

A dimensão jurisdicional do problema é objeto de uma literatura própria, que examina o alcance extraterritorial de legislações de acesso a dados e seus efeitos sobre a soberania informacional dos Estados (Irion, 2012; Roguski, 2025; Abraha, 2021). A crítica regulatória adverte que a abordagem europeia pode comprometer a adoção dos serviços de nuvem (Bania; Geradin, 2024),

ao passo que outra vertente sublinha a fragilidade da proteção oferecida pelo direito internacional a dados governamentais sob custódia de provedores estrangeiros (Roguski, 2025). No plano brasileiro, a doutrina constitucional sobre uso e compartilhamento de dados no setor público, desenvolvida a partir da Lei Geral de Proteção de Dados Pessoais (LGPD) e da jurisprudência do Supremo Tribunal Federal, fornece o enquadramento doméstico para a discussão de soberania de dados governamentais e de seus limites jurisdicionais (Brasil, 2018; Wimmer, 2021; Filgueiras; Lui, 2023).

3.4. Estudos regulatórios comparados e a lacuna identificada

Em síntese, os três eixos examinados apresentam graus distintos de consolidação: a literatura sobre riscos de nuvem governamental e sobre soberania de dados é relativamente consolidada, ao passo que a produção específica sobre informação classificada em nuvem permanece escassa. A elas somam-se a literatura de governança de tecnologias disruptivas (Filgueiras; Raymond, 2023; Papyshev; Yarime, 2023) e um conjunto crescente de instrumentos normativos nacionais. Ainda não há, porém, análise estruturada que confronte o regime brasileiro de informação classificada em nuvem (IN 8/2025) com referenciais estrangeiros. É essa lacuna que o presente artigo busca preencher, contribuindo simultaneamente com (i) a sistematização comparada de oito jurisdições, incluindo a brasileira, e (ii) a avaliação crítica do marco brasileiro à luz dessa comparação.

4. Metodologia

Esta seção descreve o desenho metodológico da pesquisa. Apresentam-se a abordagem e o tipo de estudo; os critérios de seleção dos referenciais jurisdicionais submetidos à comparação; a estrutura da matriz e seus nove critérios, distribuídos em grupos estrutural e técnico-operacional; a escala de três níveis empregada na avaliação; os procedimentos e as fontes, primárias e secundárias, incluídas as respostas a pedidos formulados com base na LAI; e as limitações reconhecidas.

4.1. Abordagem e tipo de pesquisa

A pesquisa é qualitativa, de natureza exploratória e analítica. O método principal é a pesquisa documental e bibliográfica. A técnica analítica combina o direito comparado funcional (Zweigert; Kötz, 1998), que compara institutos pela função que desempenham, e não por sua denominação formal, com a análise documental sistemática de fontes primárias (Cellard, 2008; Bowen, 2009). A construção das categorias de comparação seguiu movimento indutivo-iterativo, com triangulação de fontes para mitigar viés de interpretação (Denzin, 2009, 2012).

O estudo utilizou inteligência artificial generativa como apoio auxiliar e supervisionado na organização de ideias, na busca e sistematização de referências e na revisão de trechos do texto. A responsabilidade integral pela concepção do estudo, desenho metodológico, análise e interpretação dos dados e redação final permaneceu com o autor.

4.2. Seleção dos referenciais para comparação

Os referenciais jurisdicionais foram selecionados segundo três critérios: (i) existência de tratamento normativo publicamente disponível sobre segurança da informação para nuvem no setor público, adotado como requisito de elegibilidade; (ii) diversidade de modelos regulatórios; e (iii) relevância e influência, aferidas pela adoção como referência internacional ou pela citação frequente por outras jurisdições. Os critérios (ii) e (iii) orientaram a composição do conjunto entre candidatos elegíveis. O foco analítico permaneceu o tratamento de informação classificada, restrita ou protegida por sua sensibilidade.

O corpus comparativo resultante reúne, além do Brasil, a França, a União Europeia e os países *Five Eyes*[2]: Estados Unidos da América, Reino Unido, Austrália, Nova Zelândia e Canadá.

4.3. Construção da matriz comparativa e critérios

A comparação organiza-se em matriz estruturada por nove critérios, distribuídos em dois grupos. O Grupo A, estrutural, abrange: A1, escopo por grau de sigilo e modelo de serviço; A2, mecanismo de habilitação ou certificação de provedores; A3, responsabilidade compartilhada; A4, soberania jurisdicional e imunidade a legislação estrangeira de acesso a dados; e A5, credenciamento e verificação de pessoas. O Grupo B, técnico-operacional, abrange: B1, gerenciamento de chaves criptográficas; B2, localização de dados e estratégia de saída; B3, auditoria independente e monitoramento contínuo; e B4, segurança da cadeia de suprimentos de TIC.

4.4. Escala de avaliação

Cada critério é avaliado, por jurisdição, em escala de três níveis: previsão plena (✓) — requisito previsto com especificação técnica suficiente; previsão parcial (○) — requisito mencionado sem especificação suficiente, configurando lacuna operacional; e ausência (×) — requisito não previsto. As regras de decisão aplicadas a cada critério estão documentadas no Apêndice B. A célula reflete a previsão no nível de sensibilidade mais alto que a jurisdição autoriza publicamente em nuvem; para as jurisdições que vedam ou não publicizam o tratamento de informação classificada em nuvem, a avaliação considera, portanto, o regime do teto autorizado, e a situação específica da informação classificada é analisada no texto.

4.5. Procedimentos e fontes

As fontes primárias incluem legislação, atos normativos, normas técnicas e *frameworks* estrangeiros vigentes na data da coleta; as fontes secundárias, publicações científicas e institucionais. Como dado empírico primário, a pesquisa coletou ainda respostas a cinco pedidos formulados com base na LAI, por meio da plataforma Fala.BR, entre 24 e 25 de março de 2026, dirigidos ao GSI/PR, ao Serviço Federal de Processamento de Dados (Serpro), à Empresa de Tecnologia e Informações da Previdência S.A. (Dataprev), à Telecomunicações Brasileiras S.A. (Telebras) e à Secretaria de Governo Digital do Ministério da Gestão e Inovação em Serviços Públicos (SGD/MGI), com respostas entre 8 e 28 de abril de 2026. O pedido dirigido à Telebras foi reapresentado em maio e decidido, em sede de recurso, em 19 de junho de 2026. O protocolo (NUP), o objeto e a síntese de cada resposta são apresentados na Seção 5.2 e sistematizados no Apêndice A. A contextualização recorreu, ainda, a acórdãos do TCU. Os requisitos foram extraídos diretamente dos textos primários; quando o documento não pôde ser obtido ou não continha a informação, o fato foi registrado explicitamente.

4.6. Limitações

A pesquisa é primariamente normativa, com complementação empírica via respostas aos pedidos embasados na LAI e exame de achados de fiscalização do TCU. São limitações reconhecidas: a inacessibilidade de informações sob restrição de acesso (o que pode restringir a análise do regramento); a assimetria de detalhamento entre países; e a realização da codificação por um único pesquisador, mitigada pela triangulação de fontes e pela transparência das regras de decisão (Apêndice B), que permitem auditar e reproduzir cada atribuição. Além disso, a análise captura

[2]O bloco Five Eyes é uma aliança de compartilhamento de inteligência entre democracias ocidentais, estruturada a partir dos acordos UKUSA do pós-guerra e hoje expandida a múltiplos mecanismos cooperativos (EUA, 2024; Kerbaj, 2022).

o estado do quadro brasileiro aproximadamente seis meses após a publicação da IN 8/2025, intervalo relativamente curto. Acrescenta-se uma limitação de observabilidade: a arquitetura de credenciamento brasileira é descentralizada e a própria IN 8/2025 determina que os contratos de serviços de nuvem sejam sigilosos, de modo que as respostas a pedidos via LAI (Apêndice A) que indicam inexistência de provedores habilitados não equivalem a prova de inexistência.

5. Resultados

5.1. Quadro normativo brasileiro e requisitos de segurança da informação

O tratamento de informações classificadas em computação em nuvem pelo Poder Executivo federal submete-se a um quadro normativo de cinco níveis hierárquicos: constitucional; supralegal (tratados internacionais de direitos humanos); legal (LAI); infralegal (decretos); e de atos normativos inferiores a decreto.[3]

A Constituição (art. 5.º, XXXIII; art. 37, § 3.º, II) e os tratados internacionais de direitos humanos de que o Brasil é parte, notadamente o Pacto Internacional sobre Direitos Civis e Políticos (art. 19, § 3.º) e a Convenção Americana sobre Direitos Humanos (art. 13, § 2.º), estabelecem que o direito de acesso à informação pública pode ser restringido por lei por razões de segurança nacional (Brasil, 1988; ONU, 1966; OEA, 1969). A LAI regulamenta essa restrição e institui a classificação da informação nos graus ultrassecreto, secreto e reservado (art. 24), sem disciplinar seu tratamento em soluções de tecnologia da informação (Brasil, 2011). No plano infralegal, o Decreto n.º 7.724/2012 estabelece os procedimentos gerais de classificação e o Decreto n.º 7.845/2012 regula o credenciamento de segurança e o tratamento de informação classificada, instituindo uma governança em três níveis (Núcleo de Segurança e Credenciamento do GSI/PR e órgãos de registro níveis 1 e 2) e determinando o uso de algoritmo de Estado para os recursos criptográficos (Brasil, 2012a,b).

Nos atos inferiores a decreto, as Instruções Normativas GSI/PR n.ºs 5/2021 e 8/2025 tratam diretamente da nuvem: a IN 5/2021 vedava o tratamento de informações classificadas em qualquer modelo de nuvem (art. 17, II), vedação afastada pela nova redação que lhe deu o art. 11 da IN 8/2025, que estabeleceu o modelo vigente (Brasil, 2021, 2025b). O mecanismo de habilitação de provedores do art. 8.º da IN 8/2025 remete ao credenciamento da IN SE/CDN n.º 2/2013 e de sua Norma Complementar (NC) 01 (Brasil, 2013c,b), concebido em torno da custódia de documentos e sistemas em instalações fixas, verificadas por inspeção *in loco*.[4] Por sua vez, a IN GSI/PR n.º 3/2013 e a NC09/IN01/DSIC/GSIPR/2014 disciplinam a criptografia de informações classificadas (Brasil, 2013a, 2014). A Instrução Normativa GSI/PR n.º 10, de 3 de julho de 2026 (IN 10/2026), revogou dispositivos da IN SE/CDN n.º 2/2013 (incisos III e XI do art. 2.º e arts. 8.º a 12 e 21) e da NC01/2013 (itens 3.2, 3.10, 5, 10.1, 10.4 e 10.5 e Anexos A e B), atualizando o rito de credenciamento de pessoas naturais (Brasil, 2026b).[5]

[3] A LGPD, a PNCiber (Decreto n.º 11.856/2023), a PNSI (Decreto n.º 12.572/2025) e o PPSI (Portaria SGD/MGI n.º 9.511/2025) não integram esse quadro, por não trazerem regras diretamente aplicáveis ao tratamento de informações classificadas (Brasil, 2018, 2023a, 2025d,e).

[4] A qualificação mínima prevista na NC01/2013 não ignora o digital; alcança documentos eletrônicos, redes de dados e sistemas de TI protegidos e recursos criptográficos (item 8.5, alíneas *b*, *c*, *f* e *l*). Não obstante, existe um descompasso em sua aplicação à nuvem. A NC condiciona a habilitação à localização em área de acesso restrito e à inspeção *in loco* das instalações (itens 8.5, *a*, e 9.7), sem apresentar critérios específicos para infraestrutura virtualizada, multilocatária ou administrada por terceiros, atributos definidores da computação em nuvem (Mell; Grance, 2011; Brasil, 2013b).

[5] A IN 10/2026 não alcança as seções de habilitação de órgãos de registro e postos de controle da NC01/2013 (itens 6 a 9), que permanecem em vigor e constituem o rito a que remete o art. 8.º da IN 8/2025. É posterior, ademais, ao ciclo de pedidos de acesso à informação analisado na Seção 5.2.

Parte expressiva das disposições sobre o tratamento de informações classificadas em soluções de tecnologia da informação recorre a conceitos jurídicos indeterminados ("recursos criptográficos adequados", "mecanismos automatizados de alertas para atividades suspeitas", "alta disponibilidade", entre outros), cuja especificação técnica é transferida ao GSI/PR e aos órgãos e entidades do Poder Executivo.[6]

O Apêndice C compila os requisitos de segurança da informação do quadro brasileiro, organizados em cinco blocos funcionais. Para a análise comparativa, três opções regulatórias são especialmente relevantes: a) a exigência de habilitação do provedor como órgão de registro ou posto de controle (art. 8.º), somada ao estabelecimento no Brasil, às certificações ISO/IEC e à infraestrutura física dedicada (art. 7.º, caput, I a V), que condicionam o acesso ao mercado; b) a atribuição da auditoria de conformidade ao próprio órgão contratante (art. 9.º, caput, II); e c) a vedação de acesso do provedor ao conteúdo das informações (art. 3.º, caput, XIII), combinada à residência nacional de dados, processamento e trânsito (arts. 4.º e 5.º). A esses requisitos somam-se os da Portaria SGD/MGI n.º 5.950/2023, quais sejam classificação prévia, portabilidade, encerramento contratual com eliminação segura e propriedade exclusiva do órgão sobre dados e *logs*, de observância obrigatória no âmbito do SISP (Brasil, 2023b).

Sistematizado dessa forma, o quadro brasileiro revela-se disperso entre níveis hierárquicos e autoridades distintas (Presidência da República, GSI/PR e SGD/MGI) e fundado, em pontos críticos, em instrumentos de 2013 e 2014, anteriores à consolidação da política federal de computação em nuvem:[7] a habilitação de provedores (art. 8.º da IN 8/2025) remete ao rito da IN SE/CDN n.º 2/2013 e da NC01/2013, e a criptografia de informações classificadas é disciplinada pela IN GSI/PR n.º 3/2013 e pela NC09/2014, circunstância não alterada pela IN GSI/PR n.º 10/2026, que atualizou apenas o credenciamento de pessoas naturais (Brasil, 2026b). As implicações dessa configuração para a efetividade do quadro são examinadas na Seção 6.6.

5.2. Evidências de pedidos de acesso à informação

Os quatro achados mais relevantes dos pedidos sistematizados no Apêndice A são os seguintes. Primeiro, seis meses após a publicação da IN 8/2025, o GSI/PR informou não haver habilitado diretamente nenhum provedor nos termos do art. 8.º, tampouco ter informação sobre a habilitação por órgão de registro (Brasil, 2026c). O Serpro e a Dataprev não estão habilitados ou em processo de habilitação como órgão de registro ou posto de controle (Brasil, 2026g,a). A Telebras, por sua vez, informou estar em processo de habilitação como órgão de registro nível 2 (Brasil, 2026h). Segundo, as evidências indicam que o requisito de criptografia com algoritmo de Estado (art. 3.º, IV) não é atendido: o Serpro declarou que os algoritmos de Estado têm uso restrito e "não são amplamente disponibilizados para ambientes comerciais ou corporativos"; a Dataprev informou não oferecer o serviço de gestão de chaves criptográficas baseadas em algoritmo de Estado; e o GSI/PR confirmou que o guia técnico de recursos criptográficos previsto na NC09 (de 2013) não foi elaborado (Brasil, 2026g,a,c). Terceiro, as certificações ISO/IEC específicas para nuvem exigidas pelo art. 7.º estão ausentes nos candidatos: o Serpro possui 27001 e 27701 para alguns produtos, com 27017 e 27018 apenas em planejamento, e a Dataprev possui somente a 27001 para *data center* (Brasil, 2026g,a) (v. Seção 6.5). Quarto, a coordenação interinstitucional é falha: o GSI/PR planeja guia técnico sobre "tratamento de informações classificadas em ambiente digital" para 2026 sem data definida, ao passo que a SGD/MGI indica que a orientação complementar à IN 8/2025 está em discussão com a Controladoria-Geral da União (CGU), sem definição sobre

[6] Sobre conceitos jurídicos indeterminados, v. Di Pietro (2012).

[7] As primeiras contratações conjuntas de serviços de nuvem para o Poder Executivo federal datam de 2018 (Brasil, 2026f), e a disciplina normativa específica vigente para a contratação e o uso seguro da tecnologia é dada pela IN GSI/PR n.º 5/2021 e pela Portaria SGD/MGI n.º 5.950/2023 (Brasil, 2021, 2023b).

publicação de orientação complementar específica sobre o tratamento de informação classificada em ambientes de nuvem (Brasil, 2026c,e). Registre-se que a Telebras, em sede de recurso, deferiu parcialmente o pedido: revelou o estado de sua habilitação (item 2), mas indeferiu, sob o argumento de sigilo comercial (art. 22 da LAI), as certificações de nuvem e o número de órgãos contratantes (itens 1 e 3); a SGD/MGI, por sua vez, negou os dados agregados de maturidade do SISP (Brasil, 2026h,e).

5.3. Contexto: maturidade do SISP

Os dados disponíveis sobre a maturidade dos órgãos do SISP em segurança da informação evidenciam heterogeneidade expressiva e, em média, nível reduzido. O Ciclo 5 do PPSI 2.0 (agosto de 2025) registrou que aproximadamente 25% dos órgãos do SISP não entregaram o autodiagnóstico no prazo, e as quatro medidas de destaque do ciclo — criptografia em dados sensíveis em trânsito, designação de DPO, designação de gestor de SI e existência de PSI — constituem o mínimo de conformidade com a LGPD, patamar estruturalmente aquém das obrigações avançadas impostas pelo art. 9.º da IN 8/2025 (Brasil, 2025c). O Acórdão TCU n.º 2.387/2024 (Plenário) corrobora esse diagnóstico ao documentar heterogeneidade expressiva em governança de segurança da informação, inventário de ativos e gestão de incidentes (Brasil, 2024). A análise desse contexto de implementação ultrapassa o escopo desta investigação e constitui agenda de pesquisa futura.

5.4. Síntese dos referenciais selecionados

O Apêndice D apresenta a síntese completa dos referenciais selecionados. Os parágrafos a seguir destacam, para cada jurisdição, apenas as opções regulatórias relevantes para a análise comparada; o detalhamento normativo está sistematizado nos Apêndices C e D.

5.4.1. Brasil

A IN 8/2025 admite o tratamento de informação classificada em nuvem privada ou comunitária para os graus *reservado* e *secreto*, vedado o *ultrassecreto* em qualquer modelo, com a condição de o provedor estar habilitado como órgão de registro ou posto de controle, nos termos dos arts. 10 e 11 do Decreto n.º 7.845/2012 (Brasil, 2025b, 2012b). Com isso, o Brasil situa-se entre as jurisdições que autorizam a nuvem para o nível classificado, como Estados Unidos, Austrália e Reino Unido, em contraste com França e Nova Zelândia, cujos instrumentos o inviabilizam, e com o Canadá, que não publiciza essa possibilidade. O traço distintivo do desenho brasileiro não está, portanto, em autorizar a nuvem classificada, mas na técnica regulatória adotada: diferentemente de Estados Unidos e Austrália, que dispõem de programas próprios de certificação ou avaliação de provedores de nuvem, o Brasil não instituiu instrumento específico para esse fim.

5.4.2. Estados Unidos da América

O FedRAMP é o único programa de certificação público disponível, mas se aplica exclusivamente a dados não classificados (*baselines Low/Moderate/High*, avaliação por terceiro acreditado) (EUA, 2026). Para dados classificados, o DoD emprega o *Cloud Computing Security Requirements Guide* (CC SRG), com níveis de impacto (*impact levels*) IL2–IL6; o IL6, aplicável a dados SECRET em nuvem, combina o baseline FedRAMP High com o CNSSI 1253 Classified Information Overlay (98 controles adicionais), uso de rede SIPRNet segregada e instalações classificadas. O NIST SP 800-53 Rev. 5.2.0 constitui a base técnica dos controles aplicáveis de ambos os programas (EUA, 2014, 2025).

5.4.3. Austrália

O *Protective Security Policy Framework* (PSPF, 2025) estabelece 217 requisitos em seis domínios, incluindo modelo *Zero Trust* obrigatório (Req. 0098/0213), avaliação de propriedade, controle ou influência estrangeira como critério de seleção de provedores (Req. 0046) e criptografia pós-quântica obrigatória (Req. 0212). Nuvem privada ou comunitária é admitida apenas até *secret* (seção 15.2.1 do PSPF). O processo de habilitação de provedores exige avaliação independente, com renovação bienal, por auditor credenciado, complementado pelo *Information Security Manual* (ISM, mar. 2026) como referência técnica de controles (Austrália, 2025a, 2020, 2025b, 2026).

5.4.4. Reino Unido

O *Government Security Classifications Policy* (GSCP, 2023, atual. fev. 2025) define três níveis de classificação (*official/secret/top secret*). Para o nível OFFICIAL, o National Cyber Security Centre publica 14 princípios de segurança para nuvem (*Cloud Security Principles*), porém sem instrumento público único de certificação de provedores; o modelo para *secret* e *top secret* não é público (Reino Unido, 2023, 2021).

5.4.5. França

A *Instruction Générale Interministérielle* n.º 1300 (IGI 1300, 2021), aplicável a dados *secret* e *très secret*, impõe separação física obrigatória e proibição de acesso remoto por princípio, requisitos estruturalmente incompatíveis com qualquer arquitetura de nuvem funcional (França, 2021). Para dados *Diffusion Restreinte* e sistemas de informação sensíveis, a *Instruction Interministérielle* n.º 901 (II 901, 2015) exige certificação pelo referencial SecNumCloud v3.2, que inclui requisitos de imunidade jurídica e técnica a legislações extraterritoriais (exigência 19.6: sede na UE, capital extra-UE $\leq 24\%$ individual e $\leq 39\%$ agregado, vedação técnica de acesso por entidades extra-UE) (França, 2022, 2024). A França apresenta, assim, dois regimes distintos: vedação de nuvem para o nível classificado e exigência de SecNumCloud para o nível sensível.

5.4.6. União Europeia

O *European Cybersecurity Certification Scheme for Cloud Services* (EUCS; rascunho revisado mar. 2024) define três níveis de garantia (*Basic/Substantial/High*) e, no nível *High*, exige gestão de chaves exclusivamente pelo cliente (CKM-03.4) e avaliação por terceiro independente (CAB acreditado) (União Europeia, 2024a). O EUCS ainda não foi adotado formalmente, em razão do impasse político sobre a manutenção do requisito de soberania jurisdicional (inspirado na exigência 19.6 do SecNumCloud), removido do rascunho de 2024 e substituído por uma *International Company Profile Attestation* (ICPA) — declaração do provedor sobre as jurisdições a que está sujeito, verificada por um *Conformity Assessment Body* (CAB). A Diretiva NIS2 (2022/2555) estabelece dez medidas mínimas obrigatórias para entidades essenciais e importantes, incluindo criptografia, cadeia de suprimentos e gestão de incidentes (art. 21.2), e o Regulamento de Execução (UE) 2024/2690 operacionaliza a NIS2 com doze componentes obrigatórios de programa de gestão de chaves (KMP) (União Europeia, 2022, 2024a,b).

5.4.7. Nova Zelândia

O *New Zealand Information Security Manual* v3.9 (NZISM, abr. 2025) proíbe, por controles específicos, a acreditação e o uso de nuvem pública ou híbrida para dados *confidential*, *secret* e *top secret* (CID:7388 e CID:4802) (Nova Zelândia, 2025c). O *Protective Security Requirements* v1.0 (PSR, out. 2025) adota sistema de sete níveis de classificação (Nova Zelândia, 2025a).

5.4.8. Canadá

A *Direction on the Secure Use of Commercial Cloud Services* (SPIN 2017-01, atual. out. 2025) fixa o teto de *Protected B* para nuvem comercial. Não há norma ostensiva que discipline o tratamento de informações classificadas em nuvem. A residência de dados no Canadá é obrigatória para *Protected B/C* e *Classified* (ITPIN 2017-02) (Canadá, 2019b, 2017b,a). Mesmo os instrumentos mais recentes de soberania digital (Digital Sovereignty Framework, nov. 2025) e de criptografia pós-quântica (SPIN de PQC, out. 2025; *roadmap* ITSM.40.001) limitam-se a citar *Protected B* e abaixo, remetendo sistemas classificados ao Cyber Centre (Canadá, 2025b,d,a).

5.5. Matriz comparativa

A matriz comparativa apresentada na Tabela 1 analisa os nove critérios definidos em relação aos referenciais selecionados.

Tabela 1. Matriz comparativa dos referenciais selecionados

Critério	BR	EUA	AU	UK	FR	UE	NZ	CA
Grupo A — Estrutural								
A1: Escopo por grau de sigilo e modelo de serviço	○	✓	✓	✓	✓	✓	✓	✓
A2: Mecanismo de habilitação/certificação	○	✓	✓	○	✓	✓	✓	○
A3: Responsabilidade compartilhada	○	✓	✓	✓	✓	✓	✓	✓
A4: Soberania jurisdicional e imunidade a legislação estrangeira de acesso a dados	○	○	○	○	✓	○	×	○
A5: Credenciamento e verificação de pessoas	✓	✓	✓	✓	✓	○	✓	✓

continua...

Tabela 1. (continuação)

Critério	BR	EUA	AU	UK	FR	UE	NZ	CA
Grupo B — Técnico-operacional								
B1: Gerenciamento de chaves criptográficas	○	✓	✓	✓	✓	✓	✓	○
B2: Localização de dados e estratégia de saída	○	○	○	○	✓	✓	✓	✓
B3: Auditoria independente e monitoramento contínuo	○	✓	✓	✓	✓	✓	○	✓
B4: Segurança da cadeia de suprimentos de TIC	×	✓	✓	○	○	✓	○	○

Nota: BR = Brasil; EUA = Estados Unidos da América; AU = Austrália; UK = Reino Unido; FR = França; UE = União Europeia; NZ = Nova Zelândia; CA = Canadá. ✓ = previsão plena; ○ = previsão parcial (lacuna operacional); × = ausência (lacuna de previsão). A célula reflete a previsão no nível de sensibilidade mais alto que a jurisdição autoriza publicamente em nuvem; a situação específica da informação classificada é analisada no texto ou no Apêndice D. Células com codificação registrada conforme as regras do Apêndice B: EUA-A4 (○, com base nos requisitos funcionais do IL6, sem imunidade explícita a legislação estrangeira); UE-A4 (○, com base no rascunho de 2024 do EUCS, que substituiu a exigência de imunidade pela ICPA); CA-B3 (✓, com base na avaliação independente do rito de ATO apoiado pelo CCCS/CSE para *Protected B*). *Fonte*: Elaborada pelo autor (2026).

Os padrões de convergência, divergência e lacuna identificados na matriz são os seguintes. Em convergência, quase todas as jurisdições exigem (i) escopo diferenciado por grau de sigilo e modelo de serviço (A1; apenas BR com ○); (ii) residência de dados em território nacional ou equivalente (B2, com variação em estratégia de saída); e (iii) credenciamento de pessoas com acesso à infraestrutura (A5; BR ✓, convergente com FR, EUA, UK, AU, NZ e CA). Em divergência relevante, a soberania jurisdicional e imunidade a legislação estrangeira de acesso a dados (A4) apresenta o maior espalhamento: FR ✓ detém a proteção mais explícita (exigência 19.6 do SecNumCloud); BR, EUA, UK, AU, CA e UE ○ possuem proteção apenas parcial ou indireta (residência de dados, estabelecimento nacional, avaliação de influência estrangeira ou, no caso da UE, atestação de perfil jurisdicional) sem vedação a provedor sujeito a legislação extraterritorial; NZ × carece de proteção jurisdicional ostensiva. Em lacunas exclusivas do Brasil, destaca-se B4 × (cadeia de suprimentos).

6. Discussão

Convém, de início, delimitar o alcance da análise crítica. A viabilidade do tratamento de informação classificada em nuvem não está, em si, em questão. O caso ucraniano é ilustrativo: a migração emergencial de dados governamentais para a nuvem, às vésperas da invasão de 2022, preservou-os de ataques cinéticos e cibernéticos coordenados contra *datacenters* físicos, demonstrando que a infraestrutura local pode ser *mais* vulnerável que a nuvem distribuída (Papaleonidas, 2025; Roguski, 2025). No mesmo sentido, o levantamento de Papaleonidas (2025) junto a ministérios finlandeses registrou 85% de concordância, total ou parcial, com a proposição de que informações classificadas podem ser tratadas em nuvem desde que implementados controles adequados de cibersegurança, proteção de dados e gestão de riscos, sem identificar fator que as proíba de modo absoluto. A opção brasileira pela permissão condicionada, e não pela vedação absoluta adotada pela França e pela Nova Zelândia, é, em princípio, defensável. A análise crítica não recai, portanto, sobre a decisão de admitir a nuvem, mas sobre a adequação dos controles previstos no quadro brasileiro.

Os resultados permitem testar a hipótese deste estudo e confirmá-la. A comparação revela

que, embora apresente convergências no desenho estrutural, o quadro brasileiro tende a enunciar princípios de proteção sem a especificação técnica e a verificação independente necessárias para torná-los auditáveis. As subseções seguintes discutem, em primeiro lugar, as convergências identificadas e, em seguida, quatro lacunas de conteúdo dos requisitos. Seguem-se duas notas complementares, sobre a imprecisão do requisito de certificação e sobre a arquitetura do quadro brasileiro, e a seção encerra-se com as recomendações de aprimoramento normativo (Seção 6.7).

6.1. Convergências estruturais

Em seu desenho geral, o quadro brasileiro alinha-se aos referenciais em quatro pontos: residência de dados (arts. 4.º e 5.º da IN 8/2025), controle das chaves pelo contratante (art. 3.º, caput, V), credenciamento de pessoas (A5)[8] e delimitação do escopo por grau de sigilo, com vedação expressa ao tratamento de informação ultrassecreta em qualquer modelo de nuvem (A1), opção compatível com as jurisdições mais cautelosas. Não obstante, o quadro normativo brasileiro apresenta problemas significativos de detalhamento para a implementação das regras, conforme sustenta a análise das lacunas a seguir.

6.2. Lacuna de previsão: cadeia de suprimentos

A ausência de requisitos de cadeia de suprimentos (B4) é a lacuna de maior relevância geopolítica. Conforme Baldoni e Di Luna (2025), a soberania digital depende do acesso contínuo a capacidades tecnológicas críticas confiáveis, e a confiabilidade é atributo relacional; ou seja, um mesmo provedor pode ser confiável para uma jurisdição e não para outra. Nesse sentido, o NIST SP 800-53 Rev. 5.2.0 dos EUA (família SR), a NIS2 europeia (art. 21.2, d), o PSPF australiano (Req. 0046) e o PSR neozelandês (GOV5) impõem gestão de risco de fornecedores de TIC (EUA, 2025; União Europeia, 2022; Austrália, 2025a; Nova Zelândia, 2025b).

No caso brasileiro, os achados de fiscalização do TCU indicam que a implementação de nuvem por Dataprev e Serpro ocorre por meio de provedores de tecnologia estrangeiros expostos a legislação extraterritorial (Brasil, 2026i). O próprio Serpro informa operar sua nuvem soberana com *stacks* de fabricantes estrangeiros em seus *data centers* (Brasil, 2025f). Em linha com esse diagnóstico, Cassino (2025) destaca o risco de exposição a legislações estrangeiras como a CALEA.[9] O diagnóstico de Brasil (2026d) e Belli *et al.* (2026) qualifica essa exposição como "interdependência instrumentalizada",[10] vetor de coerção com consequências como vigilância estrangeira e estrangulamento (possibilidade de interrupção de acesso). Na contramão desse cenário, o quadro brasileiro não exige diligências sobre nacionalidade, estrutura de controle ou exposição extraterritorial desses fornecedores antes da habilitação. Soma-se, ainda, a ausência de dever de notificação análogo ao controle A.6.1 da ISO/IEC 27018 e aos controles INQ do EUCS (União Europeia, 2024a): apesar de vedar o acesso do provedor ao conteúdo das informações classificadas (art. 3.º, caput, XIII), o quadro brasileiro não o obriga a comunicar ao órgão contratante eventual determinação estrangeira de acesso, lacuna que deixa sem mitigação o risco examinado a seguir.

[8] Recentemente atualizado pela IN 10/2026, que escalona a investigação de segurança por grau de sigilo, prevê consulta à ABIN ou ao centro de inteligência da respectiva Força Armada e fixa prazos de validade da credencial de sete, cinco e três anos (reservado, secreto e ultrassecreto) (Brasil, 2026b).

[9] A *Communications Assistance for Law Enforcement Act* (CALEA), lei dos EUA de 1994, obriga operadoras de telecomunicações e fabricantes de equipamentos a conceber seus produtos e serviços com capacidade técnica de interceptação para atender a ordens de autoridades de aplicação da lei dos EUA (Cassino, 2025).

[10] Emprestando o conceito de Farrell e Newman (2019).

6.3. Soberania jurídica: residência nacional de dados *versus* alcance da legislação estrangeira

Em relação ao critério de soberania jurídica (A4), o quadro brasileiro prevê o estabelecimento do provedor no Brasil (art. 7.º, caput, I e III, da IN 8/2025) e a gestão exclusiva de chaves (art. 3.º, caput, V), que constituem proteção jurisdicional *de facto*. Não há, porém, vedação a provedores sujeitos a legislação extraterritorial nem requisito de estrutura acionária equivalente à exigência 19.6 do SecNumCloud (França, 2022).

A questão crítica em relação a esse ponto é que a localização física em território nacional não protege os dados de uma ordem de acesso emanada de jurisdição estrangeira. O *Clarifying Lawful Overseas Use of Data Act* (CLOUD Act), de 2018, ao inserir o § 2713 no Título 18 do *U.S. Code*, determina que todo provedor sujeito à jurisdição dos EUA entregue às autoridades estadunidenses os dados sob seu controle "*regardless of whether [...] located within or outside of the United States*", isto é, ainda que armazenados em *data center* situado no Brasil.

O CLOUD Act prevê uma via de contestação. O provedor pode pleitear judicialmente a invalidação da ordem quando o titular dos dados não for cidadão nem residente nos EUA e o fornecimento implicar violação da legislação de um *qualifying foreign government*, qualificação reservada aos países que celebraram com os Estados Unidos um acordo executivo nos termos da Seção 105 da lei. Caso esse acordo exista, o juiz dos EUA realiza uma análise de reciprocidade entre ordens jurídicas, ponderando o conflito entre a ordem estadunidense e a lei do país estrangeiro. Ocorre que o Brasil não celebrou tal acordo e, por isso, não se qualifica como *qualifying foreign government*. Sem essa qualificação, o provedor fica desprovido do fundamento legal que lhe permitiria opor-se à ordem. A obrigação de fornecer os dados torna-se, na prática, incondicional quanto às informações de instituições brasileiras (EUA, 2018).

A exposição brasileira não é meramente hipotética. Ao fiscalizar a nuvem de governo, o TCU identificou que os contratos da solução AWS Outposts firmados por Serpro e Dataprev preveem a divulgação de dados para cumprir "ordem válida e vinculante de órgão governamental", sem delimitar que tal autoridade deva ser brasileira (Brasil, 2026i). Essa redação admite submissão a ordens dos EUA sob o CLOUD Act; por essa razão, o TCU recomendou o aditamento da cláusula para restringi-la a autoridades nacionais.[11] Roguski (2025) sustenta que o paradigma clássico de soberania territorial é estruturalmente inadequado para funções governamentais hospedadas em infraestrutura submetida a legislação extraterritorial. Especialistas jurídicos divergem sobre se *data centers* dedicados protegem contra acesso estrangeiro (Yousuf *et al.*, 2025). A esse respeito, Dudoit e Labillois (2025) sintetizam o princípio nos seguintes termos: "*true sovereignty requires legal applicability [...] not solely physical data location*".

Nesse cenário, a residência nacional dos dados exigida pelo art. 5.º não representa mitigação jurídica suficiente. Há, porém, uma mitigação técnica: o CLOUD Act, em sua Seção 105, veda que acordos executivos imponham ao provedor a obrigação de quebrar a cifração dos dados dos clientes (§ 2523(b)(3)). Combinada com o controle das chaves pelo órgão (art. 3.º, caput, V), essa proteção neutraliza, na prática, a possibilidade de leitura compulsória do conteúdo cifrado. Essa mitigação esbarra, porém, na lacuna operacional do quadro normativo brasileiro em relação à gestão criptográfica, como abordado na subseção seguinte.

[11] O Acórdão TCU n.º 1380/2026 examina a nuvem de governo destinada a dados de acesso restrito *não classificados* (sigilo fiscal, bancário, comercial); como o regime de informação classificada da IN GSI/PR n.º 8/2025 é mais exigente, os riscos documentados no acórdão reforçam a análise desenvolvida neste artigo.

6.4. Lacunas operacionais: gerenciamento de chaves e auditoria independente

O critério de gerenciamento de chaves (B1) ilustra o padrão das lacunas operacionais. A IN 8/2025 exige gestão exclusiva de chaves criptográficas pelos órgãos de registro, vedado o armazenamento na nuvem (art. 3.º, caput, V); a IN GSI/PR n.º 5/2021 determina que o contratante utilize, "sempre que possível, chaves de encriptação baseadas em hardware" (art. 14, caput, III); e a Portaria SGD/MGI n.º 5.950/2023 exige que provedor e cliente sigam "políticas e procedimentos para o uso de criptografia, incluindo gerenciamento de chaves criptográficas", com esquema adequado ao nível de sigilo e vedação de armazenamento das chaves na nuvem (Anexo I, item 10.2, *j* e *k*). O quadro brasileiro, portanto, enuncia a custódia das chaves pelo órgão e chega a exigir a existência de uma política de gerenciamento de chaves (*key management policy* – KMP). Contudo, não define seu conteúdo mínimo, não torna o uso de *hardware security module* (HSM) obrigatório e tampouco fixa parâmetros técnicos verificáveis.

Em contraste, os referenciais comparados detalham e tornam vinculantes os mecanismos que o quadro brasileiro apenas enuncia: HSM no SecNumCloud (exigência 10.5) e no NZISM (CID:3103 e seção 17.10); KMP específico para nuvem no NZISM (CID:7462); componentes obrigatórios de KMP no Regulamento de Execução (UE) 2024/2690; e controle do material de chaveamento pelo órgão no NIST SP 800-144 (França, 2022; Nova Zelândia, 2025c; União Europeia, 2022, 2024b; EUA, 2011). Dudoit e Labillois (2025) listam, igualmente, o controle nacional da gestão de chaves criptográficas como postura mínima de uma nuvem soberana, recomendando ainda o uso de *trusted execution environments* para operações criptográficas sensíveis.

A lacuna é agravada por um problema circular na criptografia de Estado: o art. 3.º, caput, IV, da IN 8/2025 exige algoritmo de Estado, mas as empresas de TI vinculadas ao Poder Executivo federal declararam não ter acesso a esse tipo de algoritmo (Seção 5.2; Apêndice A). O êxito da IN 8/2025 parece exigir, portanto, que o Estado brasileiro supere esse óbice de implementação em aspecto crítico para a segurança da informação.

Outra assimetria aparece na auditoria independente (B3). A IN 5/2021 exige do provedor auditoria anual SOC 2, conduzida por auditor independente e acompanhada de relatórios tipo I e tipo II (art. 20, caput, XIV). A IN 8/2025, por sua vez, determina que os registros de acesso sejam objeto de auditorias periódicas por equipe independente (art. 3.º, caput, IX), mas atribui a auditoria de conformidade com a própria norma ao órgão contratante (art. 9.º, caput, II), e não a terceiro independente. A auditoria SOC 2, contudo, é um padrão genérico de controles de serviço, e não um esquema de certificação acreditado e específico, como o 3PAO do FedRAMP, o PASSI do SecNumCloud ou o IRAP australiano (EUA, 2026; França, 2022; Austrália, 2026).

Nesse contexto, a auditoria independente, ao verificar o cumprimento de requisitos, reduz a assimetria informacional entre órgão contratante e provedor e amplia a capacidade de detecção de não conformidades. A literatura identifica essa independência como condição de credibilidade dos esquemas de certificação de nuvem para governo (Papaleonidas, 2025; Ukeje; Gutierrez; Petrova, 2024). Persiste, portanto, a divergência em relação aos referenciais que vinculam a habilitação em níveis de maior sensibilidade a avaliação independente, acreditada e periódica.

6.5. Imprecisão do requisito de certificação

Cabe uma nota complementar sobre a imprecisão do requisito de certificação de provedores trazido pela IN 8/2025 (enquadrado no critério A2). O art. 7.º, caput, II, da IN exige que o provedor "possua certificação vigente" em cinco normas que, todavia, não compartilham a mesma natureza. A ABNT NBR ISO/IEC 27001 é norma de requisitos de sistema de gestão, concebida para certificação (ISO/IEC, 2018; ABNT, 2022a). As ABNT NBR ISO/IEC 27017 e 27018 são,

por designação expressa, códigos de prática de controles derivados da ISO/IEC 27002, ou seja, diretrizes, e não requisitos auditáveis como sistema de gestão (ABNT, 2016, 2021, 2022b). A ABNT NBR ISO/IEC 27701 ilustra, ademais, a instabilidade do objeto do requisito: na edição de 2019, vigente quando da publicação da IN 8/2025, era extensão da 27001, cuja certificação pressupunha (ABNT, 2019); dias depois, a edição internacional ISO/IEC 27701:2025 converteu-a em norma autônoma de sistema de gestão, certificável independentemente da 27001, condição incorporada pela edição brasileira vigente (ABNT, 2026). A ABNT NBR ISO/IEC 22237, por sua vez, é especificação de instalações e infraestruturas de *data center*, em parte publicada como especificação técnica, de natureza distinta de uma norma de sistema de gestão (ABNT, 2023). Disso decorre que a exigência não se traduz, na prática, em cinco certificações organizacionais independentes, mas, no limite, em certificado ISO/IEC 27001 de escopo estendido, incorporando os controles de 27017 e 27018; em certificado 27701 — vinculado ao primeiro sob a edição de 2019 e autônomo sob a edição vigente; e em avaliação de conformidade da instalação de *data center*. Ao equiparar, sob o mesmo comando ("possuir certificação"), objetos de naturezas distintas, a norma incorre em imprecisão técnica que pode indicar uma transposição apressada do vocabulário de certificação ao desenho do requisito.

6.6. Arquitetura normativa e efetividade

Como visto na Seção 2, conforme o paradigma DEG, a transformação digital do setor público depende menos da adoção tecnológica em si do que do desenho institucional e normativo que a sustenta (Dunleavy *et al.*, 2006; Margetts; Dunleavy, 2013; Haug; Dan; Mergel, 2024). Sob essa perspectiva, a efetividade normativa é condicionada não apenas pela completude de cada requisito, mas pelo modo como o conjunto se organiza. Três características do quadro brasileiro a comprometem.

A primeira é a dispersão da produção normativa entre níveis hierárquicos e autoridades distintas: a matéria distribui-se por decreto, instruções normativas e portaria, editados pela Presidência da República, pelo GSI/PR e pela SGD/MGI, sem instrumento de consolidação (Seção 5.1). A segunda é o descompasso entre o objeto regulado e o paradigma dos instrumentos regulatórios: a habilitação de provedores do art. 8.º da IN 8/2025 remete a um regime de credenciamento centrado em instalações físicas, cujos requisitos de TIC estão limitados a defesas perimetrais genéricas, sem critérios específicos para infraestrutura virtualizada, distribuída e administrada por terceiros (Brasil, 2013c,b). A disciplina da criptografia de informações classificadas, por sua vez, é estabelecida em atos de 2013 e 2014 (IN GSI/PR n.º 3/2013 e NC09/2014) (Brasil, 2013a, 2014). A terceira é a rigidez hierárquica: parâmetros técnicos suscetíveis de obsolescência tecnológica encontram-se fixados no Decreto n.º 7.845/2012 (ex. arts. 30-33, 38 e ss.), de modo que sua atualização depende de novo ato presidencial (Brasil, 2012b).

Essas características não são neutras quanto à efetividade. A dispersão normativa, somada ao recurso frequente a conceitos jurídicos indeterminados (Seção 5.1), transfere a especificação técnica e a implementação a órgãos e entidades de maturidade variável, sem coordenação assegurada. As respostas aos pedidos de acesso à informação revelam falhas de coordenação interinstitucional, enquanto os dados de maturidade do SISP indicam patamar médio reduzido e fortemente heterogêneo, estruturalmente aquém das obrigações da IN 8/2025. Ao delegar a concretização sem fixar parâmetros nem assegurar capacidades, a arquitetura normativa converte-se em fator de risco à segurança da informação.

6.7. Recomendações

As lacunas codificadas na matriz comparativa para o Brasil (Tabela 1) permitem tratamento a partir de soluções funcionalmente equivalentes de outras jurisdições analisadas. Propõem-se, assim, seis recomendações para o aprimoramento do quadro brasileiro. As cinco primeiras respondem, cada uma, a uma lacuna específica; a sexta, transversal, responde ao diagnóstico de arquitetura normativa desenvolvido na Seção 6.6 e inclui medidas de curto e de médio prazo.

Recomendação 1 — Especificação técnica do gerenciamento de chaves criptográficas (critério B1). Editar ato normativo complementar ou alterar a IN 8/2025 para fixar os mecanismos técnicos admissíveis de gerenciamento e custódia das chaves dos órgãos de registro, a exemplo da exigência de *hardware security modules* certificados e da definição de *key management policy* explícita, na linha do SecNumCloud, do NZISM e do NIS2 (França, 2022; Nova Zelândia, 2025c; União Europeia, 2022).

Recomendação 2 — Viabilização de criptografia de Estado ou criptografia aprovada (critério B1). Revisar a IN GSI/PR n.º 3/2013 e a Norma Complementar n.º 09/IN01/DSIC/GSIPR/2014 para difundir a implementação de criptografia de Estado ou de criptografia aprovada e definir horizonte de transição pós-quântica, em diálogo com modelos como os *ASD-Approved Cryptographic Algorithms* (AACAs) australianos e os *roadmaps* do Cyber Centre canadense (Austrália, 2026; Canadá, 2025a).

Recomendação 3 — Esquema de certificação acreditado e específico para nuvem classificada (critério A2). Instituir programa próprio de avaliação e habilitação técnica de provedores de nuvem para informações classificadas, conduzido por terceiro independente acreditado, com escopo técnico próprio, periodicidade de reavaliação e publicidade da lista de provedores habilitados. Os modelos do FedRAMP/3PAO (EUA), do SecNumCloud/PASSI (França) e do IRAP (Austrália) fornecem parâmetros funcionalmente equivalentes (EUA, 2026; França, 2022; Austrália, 2020).

Recomendação 4 — Fortalecimento da proteção jurisdicional (critério A4). Incorporar, na IN 8/2025 ou em ato complementar, controles de soberania jurídica destinados a mitigar o risco de acesso por jurisdição estrangeira: (i) vedação à habilitação de provedores sujeitos a legislação extraterritorial sem mecanismos contratuais e técnicos de oposição, à semelhança da exigência 19.6 do SecNumCloud (França, 2022); (ii) dever de notificação ao órgão contratante diante de qualquer requisição governamental estrangeira de acesso, à semelhança do controle A.6.1 da ISO/IEC 27018 e dos controles INQ do EUCS (União Europeia, 2024a); e (iii) exigência de cláusula contratual restringindo a divulgação a ordens emanadas de autoridades brasileiras, alinhada à recomendação do Acórdão TCU n.º 1380/2026 (Brasil, 2026i).

Recomendação 5 — Requisitos de segurança da cadeia de suprimentos de TIC (critério B4). Estabelecer requisitos explícitos de gestão de risco de fornecedores de TIC aplicáveis à habilitação de provedores e à composição de sua infraestrutura, incluindo diligência sobre nacionalidade, estrutura de controle e exposição extraterritorial. Os referenciais comparados oferecem modelos consolidados: família SR do NIST SP 800-53 Rev. 5.2.0, art. 21.2, alínea *d*, da NIS2, Req. 0046 do PSPF australiano e GOV 5 do PSR neozelandês (EUA, 2025; União Europeia, 2022; Austrália, 2026; Nova Zelândia, 2025c).

Recomendação 6 — Revisão da arquitetura normativa (transversal). No curto prazo, articular formalmente a IN 8/2025 com a Portaria SGD/MGI n.º 5.950/2023, por ato conjunto ou remissão expressa, integrando, no contexto de informações classificadas, os requisitos de classificação prévia, portabilidade, encerramento contratual com eliminação segura e propriedade exclusiva do órgão sobre dados e *logs*. Em médio prazo: (i) revisar o Decreto n.º 7.845/2012 para

que reserve ao nível de decreto os princípios de credenciamento e a governança institucional, remetendo a atos infralegais a especificação de parâmetros técnicos suscetíveis de evolução tecnológica; (ii) integrar e atualizar as demais normas infralegais aplicáveis (IN SE/CDN n.º 2/2013 e INs GSI/PR n.º 3/2013 e n.º 8/2025; NC01/2013 e NC09/2014) e harmonizá-las em relação ao tratamento de informações classificadas em ambientes de nuvem; e (iii) consolidar os controles técnicos aplicáveis e vinculá-los ao grau de classificação em manual único, a exemplo do *Information Security Manual* (ISM) australiano e do *New Zealand Information Security Manual* (NZISM), ambos mantidos por autoridade técnica e submetidos a ciclos regulares de revisão (Austrália, 2026; Nova Zelândia, 2025c).

As recomendações não exigem execução simultânea. As de natureza infralegal e escopo pontual (Recomendações 1, 2, 4 e 5) e o item de curto prazo da Recomendação 6 podem ser adotadas por ato do GSI/PR ou por ato conjunto, sem alteração de decreto. A Recomendação 3 e o item de médio prazo da Recomendação 6 pressupõem decisão mais abrangente sobre o desenho institucional.

7. Conclusões

A análise comparativa entre o quadro normativo brasileiro e os referenciais de sete jurisdições selecionadas confirmou a hipótese: o Brasil apresenta lacunas em requisitos críticos de segurança da informação para o tratamento de informações classificadas em computação em nuvem. No grupo estrutural, há proteção jurisdicional apenas indireta diante de legislações extraterritoriais, notadamente o CLOUD Act. No eixo técnico-operacional, há ausência de previsão sobre cadeia de suprimentos de TIC e insuficiência na especificação dos mecanismos de gerenciamento de chaves. Além disso, o requisito de criptografia de Estado mostra-se, segundo as respostas obtidas via LAI, sujeito a óbices de implementação, aspecto que excede o problema de previsão normativa e remete a uma agenda mais ampla de capacidade institucional. O mecanismo de auditoria é limitado ao padrão genérico SOC 2 e à autoauditoria de conformidade pelo órgão contratante, sem equivalente à auditoria independente do 3PAO estadunidense, do PASSI francês ou do IRAP australiano.

O quadro brasileiro afirma princípios de proteção sem fixar os parâmetros técnicos e os mecanismos de verificação independente que permitiriam aferi-los. Em termos teóricos, essa é a distinção entre soberania formal e soberania operacional (Dudoit; Labillois, 2025): a primeira reside no enunciado normativo; a segunda, na capacidade efetiva e demonstrável de proteger a informação classificada em ambiente cuja segurança possa ser auditada. Esse é um déficit de arquitetura normativa: a IN 8/2025 se inseriu em arranjo fragmentado que transfere a especificação e a implementação a órgãos e entidades de maturidade variável. A insuficiência de parâmetros e de verificação independente pode ser lida, portanto, como uma propriedade de um desenho institucional que ainda não acompanha a ambição de soberania enunciada pelo governo brasileiro.

A IN 8/2025 representa, ainda assim, avanço relevante ao instituir, pela primeira vez no Brasil, um regime jurídico próprio para o tratamento de informações classificadas em nuvem. Sua maturação, contudo, depende da superação das lacunas aqui identificadas. Sem a especificação técnica, sem um esquema de verificação independente e sem a articulação institucional necessária, o regime permanece no plano da soberania formal: enunciada, mas ainda não efetiva.

7.1. Trabalhos futuros

A análise abre quatro frentes de pesquisa. A primeira é a investigação empírica da capacidade técnica e organizacional dos provedores candidatos, em especial das empresas públicas de TIC,

à luz dos requisitos do quadro brasileiro. A segunda é o estudo da maturidade institucional dos órgãos e entidades do Poder Executivo federal, em especial do SISP, e de sua capacidade de implementar esses requisitos. A terceira é o acompanhamento do processo de adoção formal do EUCS pela União Europeia e de seus impactos sobre modelos de nuvem soberana adotados no Sul Global, com possíveis implicações para o Brasil. Por fim, a quarta é o uso da metodologia desenvolvida para expandir a comparação, sugerindo-se a inclusão de outras jurisdições do Sul Global, em especial dos países do BRICS+. Em conjunto, essas frentes permitirão expandir o estudo comparativo da previsão normativa e avançar para o estudo de sua efetividade.

Referências

ABD AL GHAFFAR, Hedaia-t-Allah Nabil. Government cloud computing and national security. **Review of Economics and Political Science**, v. 9, n. 2, p. 116–133, 2020. DOI: 10.1108/reps-09-2019-0125. Acesso em: 28 mar. 2026.

ABRAHA, Halefom H. Law enforcement access to electronic evidence across borders: mapping policy approaches and emerging reform initiatives. **International Journal of Law and Information Technology**, v. 29, n. 2, p. 118–153, 2021. DOI: 10.1093/ijlit/eaab001. Acesso em: 28 mar. 2026.

ALEXY, Robert. **Teoria dos direitos fundamentais**. São Paulo: Malheiros, 2014. Tradução de Virgílio Afonso da Silva.

ALI, Omar *et al.* Assessing information security risks in the cloud: A case study of Australian local government authorities. **Government Information Quarterly**, v. 37, n. 1, p. 101419, 2020. DOI: 10.1016/j.giq.2019.101419.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **ABNT ISO/IEC TS 27100:2025 — Tecnologia da informação: segurança cibernética: visão geral e conceitos**. 1. ed. Especificação Técnica. Rio de Janeiro, 2025. 21 p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **ABNT NBR ISO/IEC 22237-1:2023: Tecnologia da informação — Instalações e infraestrutura de data center — Parte 1: Conceitos gerais**. Rio de Janeiro, jun. 2023.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **ABNT NBR ISO/IEC 27001:2022: Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos**. Rio de Janeiro, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **ABNT NBR ISO/IEC 27002:2022: Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação**. Rio de Janeiro, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **ABNT NBR ISO/IEC 27017:2016: Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação com base ABNT NBR ISO/IEC 27002 para serviços em nuvem**. Rio de Janeiro, jul. 2016.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **ABNT NBR ISO/IEC 27018:2021: Tecnologia da informação — Técnicas de segurança — Código de prática**

para proteção de dados pessoais (DP) em nuvens públicas que atuam como operadores de DP. 2. ed. Rio de Janeiro, mar. 2021.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **ABNT NBR ISO/IEC 27032:2024 — Segurança cibernética: diretrizes para segurança na internet**. 2. ed. Norma Brasileira. Rio de Janeiro, 2024. 34 p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **ABNT NBR ISO/IEC 27701:2019: Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes**. Norma técnica. Rio de Janeiro, 2019. Edição vigente à época da publicação da IN GSI/PR n.º 8/2025; substituída pela ABNT NBR ISO/IEC 27701:2026.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **ABNT NBR ISO/IEC 27701:2026: Segurança da informação, segurança cibernética e proteção da privacidade — Sistemas de gestão da privacidade da informação — Requisitos e orientações**. Norma técnica. Rio de Janeiro, 2026. Internaliza a ISO/IEC 27701:2025 (14 out. 2025), que converteu a norma em padrão autônomo de sistema de gestão, certificável independentemente da ISO/IEC 27001.

AUSTRÁLIA. **Australian Government Protective Security Policy Framework (PSPF) Release 2025**. Canberra: Attorney-General's Department, 2025. 165 p. Disponível em: https://www.protectivesecurity.gov.au. Acesso em: 26 abr. 2026.

AUSTRÁLIA. **IRAP Common Assessment Framework. Version 1.0**. Canberra: Australian Signals Directorate, abr. 2025. Disponível em: https://www.cyber.gov.au/irap. Acesso em: 26 abr. 2026.

AUSTRÁLIA. **IRAP Policy and Procedures**. Canberra: Australian Signals Directorate, nov. 2020. Disponível em: https://www.cyber.gov.au/irap. Acesso em: 26 abr. 2026.

AUSTRÁLIA. AUSTRALIAN SIGNALS DIRECTORATE; AUSTRALIAN CYBER SECURITY CENTRE. **Information Security Manual (ISM)**. Canberra, mar. 2026. Versão: março 2026. Disponível em: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism. Acesso em: 11 abr. 2026.

BALDONI, Roberto; DI LUNA, Giuseppe. Sovereignty in the digital era: the quest for continuous access to dependable technological capabilities. **IEEE Security & Privacy**, v. 23, n. 1, p. 91–96, 2025. DOI: 10.1109/MSEC.2024.3500192. Acesso em: 28 mar. 2026.

BANIA, Konstantina; GERADIN, Damien. The regulation of cloud computing: why the European Union failed to get it right. **Information & Communications Technology Law**, v. 33, n. 1, p. 99–113, 2024. Open Access. Published online 10 Oct 2023. DOI: 10.1080/13600834.2023.2260687.

BANNISTER, Frank; CONNOLLY, Regina. Trust and transformational government: a proposed framework for research. **Government Information Quarterly**, Elsevier, v. 28, n. 2, p. 137–147, 2011. DOI: 10.1016/j.giq.2010.06.010.

BELLI, Luca *et al.* **Soberania Digital e Inteligência Artificial no Brasil: rumo à autonomia tecnológica**. 1. ed. Rio de Janeiro: Lumen Juris, 2026. p. 300. ISBN 978-85-519-3956-7.

BOWEN, Glenn A. Document Analysis as a Qualitative Research Method. **Qualitative Research Journal**, v. 9, n. 2, p. 27–40, 2009. DOI: 10.3316/QRJ0902027.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 14 mar. 2026.

BRASIL. **Decreto n.º 10.222, de 5 de fevereiro de 2020: aprova a Estratégia Nacional de Segurança Cibernética (E-Ciber)**. Brasília, DF: Presidência da República, fev. 2020. Diário Oficial da União, seção 1. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm. Acesso em: 14 mar. 2026.

BRASIL. **Decreto n.º 12.573, de 4 de agosto de 2025: institui a Estratégia Nacional de Cibersegurança (E-Ciber)**. Brasília, DF: Presidência da República, ago. 2025. Diário Oficial da União, seção 1. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/d12573.htm. Acesso em: 14 mar. 2026.

BRASIL. **Lei n.º 12.527, de 18 de novembro de 2011. Regula o acesso a informações**. Brasília, DF: Presidência da República, 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 14 mar. 2026.

BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 mar. 2026.

BRASIL. EMPRESA DE TECNOLOGIA E INFORMAÇÕES DA PREVIDÊNCIA. **Resposta ao pedido de acesso à informação NUP 36783.010932/2026-95**. Brasília: Dataprev, 2026. Fala.BR — Plataforma Integrada de Ouvidoria e Acesso à Informação, 9 abr. 2026.

BRASIL. GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA. **Instrução Normativa GSI/PR n.º 10, de 3 de julho de 2026. Estabelece os procedimentos para o credenciamento de segurança de pessoas naturais para o tratamento de informação classificada em grau de sigilo**. Brasília, DF: GSI/PR, 2026. Diário Oficial da União, seção 1. Edição 124, Seção 1, p. 6–20, 6 jul. 2026.

BRASIL. GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA. **Instrução Normativa GSI/PR n.º 3, de 6 de março de 2013. Dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal**. Brasília, DF: GSI/PR, 2013. Diário Oficial da União: seção 1, Brasília, DF, 2013.

BRASIL. GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA. **Instrução Normativa GSI/PR n.º 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**. Brasília, DF: GSI/PR, 2021. Diário Oficial da União: seção 1, Brasília, DF, 31 ago. 2021. Art. 17, II, com redação dada pela IN GSI/PR n.º 8/2025. Acesso em: 14 mar. 2026.

BRASIL. GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA. **Instrução Normativa GSI/PR n.º 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**. Brasília, DF: GSI/PR, 2025. Diário Oficial da União: seção 1, Brasília, DF, 7 out. 2025. Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-gsi/pr-n-8-de-6-de-outubro-de-2025-660716869. Acesso em: 14 mar. 2026.

BRASIL. GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA. **Norma Complementar n.º 01/IN02/NSC/GSI/PR, de 27 de junho de 2013. Disciplina o credenciamento de segurança de pessoas naturais, órgãos e entidades públicas e privadas para o tratamento de informações classificadas**. Brasília, DF: GSI/PR, 2013. Homologada pela Portaria GSI/PR n.º 19, de 27 de junho de 2013. Itens 3.2, 3.10, 5, 10.1, 10.4, 10.5 e Anexos A e B revogados pela IN GSI/PR n.º 10/2026.

BRASIL. GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA. **Norma Complementar n.º 09/IN01/DSIC/GSIPR, Revisão 02. Estabelece orientações específicas para o uso de recursos criptográficos em Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta**. Brasília, DF: GSI/PR, 2014. Homologada pela Portaria GSI/PR n.º 23, de 15 de julho de 2014.

BRASIL. GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA. **Resposta ao pedido de acesso à informação NUP 00137.002849/2026-10**. Brasília: GSI/PR, 2026. Fala.BR — Plataforma Integrada de Ouvidoria e Acesso à Informação, 24 abr. 2026.

BRASIL. MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO; CENTRO DE GESTÃO E ESTUDOS ESTRATÉGICOS. **Soberania Digital no Brasil: diagnóstico, desafios e caminhos sob a perspectiva da Ciência, Tecnologia e Inovação (Sumário Executivo Estendido)**. Brasília, 2026. 14 p.

BRASIL. MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS. **75% dos órgãos federais entregam autodiagnóstico e plano de trabalho voltado para privacidade e segurança da informação**. Brasília, DF: MGI, 2025. Disponível em: https://www.gov.br/gestao/pt-br/assuntos/noticias/2025/agos/75-dos-orgaos-federais-entregam-autodiagnostico-e-plano-de-trabalho-voltado-para-privacidade-e-seguranca-da-informacao. Acesso em: 18 abr. 2026.

BRASIL. MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS. **Resposta ao pedido de acesso à informação NUP 18002.003987/2026-15**. Brasília: MGI, 2026. Fala.BR — Plataforma Integrada de Ouvidoria e Acesso à Informação, 28 abr. 2026.

BRASIL. PRESIDÊNCIA DA REPÚBLICA. **Decreto n.º 11.856, de 26 de dezembro de 2023. Institui a Política Nacional de Cibersegurança (PNCiber) e o Comitê Nacional de Cibersegurança**. Brasília, DF: Presidência da República, 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11856.htm. Acesso em: 14 mar. 2026.

BRASIL. PRESIDÊNCIA DA REPÚBLICA. **Decreto n.º 12.572, de 4 de agosto de 2025. Institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação no âmbito da administração pública federal**. Brasília, DF: Presidência da República, 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/d12572.htm. Acesso em: 14 mar. 2026.

BRASIL. PRESIDÊNCIA DA REPÚBLICA. **Decreto n.º 7.724, de 16 de maio de 2012. Regulamenta a Lei n.º 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações**. Brasília, DF: Presidência da República, 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/d7724.htm. Acesso em: 14 mar. 2026.

BRASIL. PRESIDÊNCIA DA REPÚBLICA. **Decreto n.º 7.845, de 14 de novembro de 2012. Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo**. Brasília, DF: Presidência da República, 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/d7845.htm. Acesso em: 14 mar. 2026.

BRASIL. SECRETARIA DE GOVERNO DIGITAL. **Computação em Nuvem no Governo Federal**. SGD/MGI. 2026. Disponível em: https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/estrategias-e-politicas-digitais/computacao-em-nuvem. Acesso em: 26 abr. 2026.

BRASIL. SECRETARIA DE GOVERNO DIGITAL. **O que é a diretriz "cloud first" da SGD para o Sisp?** Governo Federal do Brasil. 2022. Disponível em: https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/estrategias-e-politicas-digitais/computacao-em-nuvem/o-que-e-a-diretriz-cloud-first-da-sgd-para-o-sisp. Acesso em: 20 abr. 2026.

BRASIL. SECRETARIA DE GOVERNO DIGITAL; MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS. **Portaria SGD/MGI n.º 5.950, de 26 de outubro de 2023. Estabelece diretrizes para contratação de serviços de computação em nuvem pelos órgãos e entidades integrantes do SISP**. Brasília, DF: SGD/MGI, 2023. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-5.950-de-26-de-outubro-de-2023. Acesso em: 14 mar. 2026.

BRASIL. SECRETARIA DE GOVERNO DIGITAL; MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS. **Portaria SGD/MGI n.º 9.511, de 28 de outubro de 2025. Institui o Programa de Privacidade e Segurança da Informação no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional, que possuem unidades que integram o Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo federal.** Brasília: SGD/MGI, 2025. Diário Oficial da União, seção 1. Edição 208, Seção 1, p. 91, 31 out. 2025.

BRASIL. SECRETARIA EXECUTIVA DO CONSELHO DE DEFESA NACIONAL. **Instrução Normativa SE/CDN n.º 2, de 5 de fevereiro de 2013. Dispõe sobre o credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal**. Brasília, DF: SE/CDN, 2013. Diário Oficial da União: seção 1, Brasília, DF, 2013. Arts. 2.º, III e XI, 8.º a 12 e 21 revogados pela IN GSI/PR n.º 10/2026.

BRASIL. SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS. **Nuvem Soberana: a visão que virou política de Estado**. Brasília, DF: Serpro, 2025. Disponível em: https://www.serpro.gov.br/arquivos/nuvemsoberana-esq.pdf. Acesso em: 18 abr. 2026.

BRASIL. SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS. **Resposta ao pedido de acesso à informação NUP 18870.000928/2026-58**. Brasília: Serpro, 2026. Fala.BR — Plataforma Integrada de Ouvidoria e Acesso à Informação, 8 abr. 2026.

BRASIL. TELECOMUNICAÇÕES BRASILEIRAS S.A. (TELEBRAS). **Resposta a recurso de primeira instância no pedido de acesso à informação NUP 00132.000075/2026-32 (Memorando TLB-MEM-2026/01112)**. Brasília: Telebras, 2026. Fala.BR — Plataforma Integrada de Ouvidoria e Acesso à Informação, 19 jun. 2026.

BRASIL. TRIBUNAL DE CONTAS DA UNIÃO. **Acórdão n.º 1380/2026 — Plenário (TC 008.857/2025-3): acompanhamento da soberania de dados na implementação da nuvem de governo**. Brasília: TCU, 2026. Relator: Min. Antonio Anastasia. Sessão de 27 maio 2026, Ata 19/2026.

BRASIL. TRIBUNAL DE CONTAS DA UNIÃO. **Acórdão n.º 2.387/2024 — Plenário. Auditoria de conformidade sobre segurança da informação nos órgãos do SISP**. Brasília, DF: TCU, 2024. Disponível em: https://pesquisa.apps.tcu.gov.br/documento/acordao-completo/*/NUMACORDAO:2387%20ANOACORDAO:2024%20COLEGIADO:%22Plen%C3%A1rio%22/DTRELEVANCIA%20desc%2C%20NUMACORDAOINT%20desc/0. Acesso em: 18 abr. 2026.

BRATTON, Benjamin H. **The Stack: On Software and Sovereignty**. Cambridge, MA: MIT Press, 2015. (Software Studies).

CANADÁ. CANADIAN CENTRE FOR CYBER SECURITY. **IT Security Risk Management: A Lifecycle Approach (ITSG-33)**. Ottawa: Communications Security Establishment / Canadian Centre for Cyber Security, 2012. Disponível em:

https://www.cyber.gc.ca/en/guidance/it-security-risk-management-lifecycle-approach-itsg-33. Acesso em: 20 maio 2026.

CANADÁ. CANADIAN CENTRE FOR CYBER SECURITY. **Roadmap for the Migration to Post-Quantum Cryptography for the Government of Canada (ITSM.40.001)**. Ottawa: Communications Security Establishment / Canadian Centre for Cyber Security, 2025. Publicado em 23 jun. 2025; orientativo; sistemas non-classified. Disponível em: https://www.cyber.gc.ca/en/guidance/roadmap-migration-post-quantum-cryptography-government-canada-itsm40001. Acesso em: 14 jun. 2026.

CANADÁ. TREASURY BOARD OF CANADA SECRETARIAT. **Digital Sovereignty: A Framework to Improve Digital Readiness of the Government of Canada**. Ottawa: Treasury Board of Canada Secretariat, 2025. Publicado em 12 nov. 2025; escopo limitado a Protected B e abaixo. Disponível em: https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/digital-sovereignty/digital-sovereignty-framework-improve-digital-readiness.html. Acesso em: 14 jun. 2026.

CANADÁ. TREASURY BOARD OF CANADA SECRETARIAT. **Direction for Electronic Data Residency (ITPIN 2017-02)**. Ottawa: Treasury Board of Canada Secretariat, 2017. Disponível em: https://publications.gc.ca/collections/collection_2018/sct-tbs/BT22-210-2018-eng.pdf. Acesso em: 20 maio 2026.

CANADÁ. TREASURY BOARD OF CANADA SECRETARIAT. **Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice (SPIN) 2017-01**. Ottawa: Treasury Board of Canada Secretariat, 2017. Atualizada em out. 2025. Disponível em: https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/direction-secure-use-commercial-cloud-services-spin.html. Acesso em: 20 maio 2026.

CANADÁ. TREASURY BOARD OF CANADA SECRETARIAT. **Directive on Security Management**. Ottawa: Treasury Board of Canada Secretariat, 2019. Disponível em: https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32611. Acesso em: 20 maio 2026.

CANADÁ. TREASURY BOARD OF CANADA SECRETARIAT. **Directive on Security Screening**. Ottawa: Treasury Board of Canada Secretariat, 2025. Substitui o Standard on Security Screening. Disponível em: https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32805. Acesso em: 20 maio 2026.

CANADÁ. TREASURY BOARD OF CANADA SECRETARIAT. **Government of Canada Cloud Guardrails**. Ottawa: Treasury Board of Canada Secretariat, 2024. atualizado jan. 2024.

Disponível em: https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32787&section=html. Acesso em: 20 maio 2026.

CANADÁ. TREASURY BOARD OF CANADA SECRETARIAT. **Government of Canada Cloud Security Risk Management Approach and Procedures**. Ottawa: Treasury Board of Canada Secretariat, 2018. atualizado out. 2025. Disponível em: https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/cloud-security-risk-management-approach-procedures.html. Acesso em: 20 maio 2026.

CANADÁ. TREASURY BOARD OF CANADA SECRETARIAT. **Government of Canada White Paper: Data Sovereignty and the Public Cloud**. Ottawa: Treasury Board of Canada Secretariat, 2018. ISBN 978-0-660-27233-7. Disponível em: https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/digital-sovereignty/gc-white-paper-data-sovereignty-public-cloud.html. Acesso em: 20 maio 2026.

CANADÁ. TREASURY BOARD OF CANADA SECRETARIAT. **Migrating the Government of Canada to Post-Quantum Cryptography: Security Policy Implementation Notice**. Ottawa: Treasury Board of Canada Secretariat, 2025. Em vigor desde 9 out. 2025; escopo até Protected B; sistemas classified remetidos ao Cyber Centre. Disponível em: https://www.canada.ca/en/government/system/digital-government/policies-standards/spin/migrating-government-canada-post-quantum-cryptography.html. Acesso em: 14 jun. 2026.

CANADÁ. TREASURY BOARD OF CANADA SECRETARIAT. **Policy on Government Security**. Ottawa: Treasury Board of Canada Secretariat, 2019. Atualizada em jan. 2025. Disponível em: https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=16578. Acesso em: 20 maio 2026.

CANADÁ. TREASURY BOARD OF CANADA SECRETARIAT. **Policy on Service and Digital; Directive on Service and Digital**. Ottawa: Treasury Board of Canada Secretariat, 2025. Diretiva atualizada em out. 2025; Policy id=32603, Directive id=32601. Disponível em: https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32601. Acesso em: 20 maio 2026.

CASSINO, João Francisco. **Soberania Fatiada: Controle das Infraestruturas e Subordinação da Autoridade Pública no Mundo Digital**. 2025. Tese (Doutorado) – Universidade Federal do ABC (UFABC) — Programa de Pós-Graduação em Ciências Humanas e Sociais, Santo André. Orientador: Prof. Dr. Sérgio Amadeu da Silveira.

CELLARD, André. A análise documental. *In:* POUPART, Jean *et al.* (ed.). **A pesquisa qualitativa: enfoques epistemológicos e metodológicos**. Tradução: Ana Cristina Nasser. Petrópolis, RJ: Vozes, 2008. (Coleção Sociologia). p. 295–316.

CHRISTAKIS, Théodore. **“European Digital Sovereignty”: successfully navigating between the “Brussels Effect” and Europe’s quest for strategic autonomy**. Rochester, NY: SSRN, dez. 2020. SSRN — Studies on Digital Governance (preprint; not peer reviewed). Disponível em: https://ssrn.com/abstract=3748098. Acesso em: 28 mar. 2026.

CHRISTAKIS, Theodore; TERPAN, Fabien. EU–US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options. **International Data Privacy Law**, v. 11, n. 2, p. 81–109, 2021. DOI: 10.1093/idpl/ipaa022. Acesso em: 28 mar. 2026.

DENZIN, Norman K. Strategies of Multiple Triangulation. *In:* THE Research Act: A Theoretical Introduction to Sociological Methods. New Brunswick, NJ: Transaction Publishers, 2009. cap. 12, p. 297–313. ISBN 978-0-202-36248-9.

DENZIN, Norman K. Triangulation 2.0. **Journal of Mixed Methods Research**, v. 6, n. 2, p. 80–88, 2012. DOI: 10.1177/1558689812437186.

DI PIETRO, Maria Sylvia Zanella. **Discricionariedade Administrativa na Constituição de 1988**. 3. ed. São Paulo: Atlas, 2012.

DUDOIT, Alain; LABILLOIS, Tony. **Digital Sovereignty and Federalism: Data Interoperability and AI Governance**. Montreal, dez. 2025. Série *Pour réflexion*. DOI: 10.54932/DNAN8237. Disponível em: https://cirano.qc.ca/files/publications/2025PR-12.pdf. Acesso em: 28 mar. 2026.

DUNLEAVY, Patrick *et al.* **Digital Era Governance: IT Corporations, the State, and E-Government**. Oxford: Oxford University Press, 2006. ISBN 978-0-19-929619-4. DOI: 10.1093/acprof:oso/9780199296194.001.0001.

DWORKIN, Ronald. **Levando os direitos a sério**. São Paulo: Martins Fontes, 2002. Tradução de Nelson Boeira.

ESTADOS UNIDOS DA AMÉRICA (EUA). **Clarifying Lawful Overseas Use of Data Act (CLOUD Act). In: Consolidated Appropriations Act, 2018 (H.R. 1625), Division V**. Washington, DC: U.S. Congress, 2018. Codificado em 18 U.S.C. §§ 2523, 2713. Assinado em 23 mar. 2018. Disponível em: https://www.justice.gov/d9/pages/attachments/2019/04/09/cloud_act.pdf. Acesso em: 11 abr. 2026.

ESTADOS UNIDOS DA AMÉRICA (EUA). COMMITTEE ON NATIONAL SECURITY SYSTEMS. **Security categorization and control selection for National Security Systems. CNSSI No. 1253**. Fort Meade, MD, 2014. Atualizado em ago. 2022. Disponível em: https://www.dcsa.mil/portals/91/documents/ctp/nao/CNSSI_No1253.pdf. Acesso em: 11 abr. 2026.

ESTADOS UNIDOS DA AMÉRICA (EUA). GENERAL SERVICES ADMINISTRATION. **FedRAMP: Federal Risk and Authorization Management Program**. Washington, DC:

General Services Administration, 2026. Atualização contínua. Disponível em: https://www.fedramp.gov. Acesso em: 11 abr. 2026.

ESTADOS UNIDOS DA AMÉRICA (EUA). NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Guidelines on security and privacy in public cloud computing. NIST Special Publication 800-144**. Gaithersburg, MD, dez. 2011. Disponível em: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-144.pdf. Acesso em: 11 abr. 2026.

ESTADOS UNIDOS DA AMÉRICA (EUA). NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Security and privacy controls for information systems and organizations. NIST Special Publication 800-53, Revision 5.2.0**. Gaithersburg, MD, 2025. Arquivo JSON de referência datado de 27 abr. 2026. Disponível em: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final. Acesso em: 11 abr. 2026.

ESTADOS UNIDOS DA AMÉRICA (EUA). OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE. **Five Eyes Intelligence Oversight and Review Council (FIORC)**. 2024. Disponível em: https://www.dni.gov/index.php/ncsc-how-we-work/217-about/organization/icig-pages/2660-icig-fiorc. Acesso em: 17 jun. 2026.

FARRELL, Henry; NEWMAN, Abraham L. Weaponized Interdependence: How Global Economic Networks Shape State Coercion. **International Security**, v. 44, n. 1, p. 42–79, 2019. DOI: 10.1162/isec_a_00351. Disponível em: https://doi.org/10.1162/isec_a_00351. Acesso em: 17 jun. 2026.

FILGUEIRAS, Fernando; LUI, Lizandro. Designing Data Governance in Brazil: An Institutional Analysis. **Policy Design and Practice**, v. 6, n. 1, p. 41–56, 2023. DOI: 10.1080/25741292.2022.2065065. Disponível em: https://doi.org/10.1080/25741292.2022.2065065. Acesso em: 17 jun. 2026.

FILGUEIRAS, Fernando; RAYMOND, Anjanette. Designing Governance and Policy for Disruptive Digital Technologies. **Policy Design and Practice**, v. 6, n. 1, p. 1–13, 2023. DOI: 10.1080/25741292.2022.2162241. Disponível em: https://doi.org/10.1080/25741292.2022.2162241. Acesso em: 17 jun. 2026.

FRANÇA. AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION. **Prestataires de services d'informatique en nuage (SecNumCloud): référentiel d'exigences. Version 3.2**. Paris, mar. 2022. Disponível em: https://cyber.gouv.fr/publications/prestataires-de-services-dinformatique-en-nuage-secnumcloud-referentiel-dexigences. Acesso em: 11 abr. 2026.

FRANÇA. AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION. **Recommandations pour l'hébergement dans le cloud des systèmes d'information sensibles. Version 1.0**. Paris, jul. 2024. ISBN 978-2-11-167174-4. Disponível em: https://cyber.gouv.fr/publications/recommandations-pour-

lhebergement-dans-le-cloud-des-systemes-dinformation-sensibles. Acesso em: 11 abr. 2026.

FRANÇA. SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE. **Instruction générale interministérielle n.º 1300/SGDSN/PSE/PSD sur la protection du secret de la défense nationale**. Paris: SGDSN, ago. 2021. Disponível em: https://cyber.gouv.fr/reglementation/cybersecurite-systemes-dinformation/protection-du-secret/instruction-generale-interministerielle-n1300/. Acesso em: 11 abr. 2026.

HAUG, Nathalie; DAN, Sorin; MERGEL, Ines. Digitally-induced change in the public sector: a systematic review and research agenda. **Public Management Review**, v. 26, n. 7, p. 1963–1987, 2024. DOI: 10.1080/14719037.2023.2234917.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 27000:2018 — Information technology — Security techniques — Information security management systems — Overview and vocabulary**. 5. ed. International Standard. Geneva, 2018. 27 p.

IRION, Kristina. Government Cloud Computing and National Data Sovereignty. **Policy & Internet**, v. 4, n. 3-4, p. 40–71, 2012. DOI: 10.1002/poi3.10.

JANSSEN, Marijn; JOHA, Anton. Challenges for adopting cloud-based software as a service (SaaS) in the public sector. *In:* ECIS 2011 — European Conference on Information Systems. Helsinki: Association for Information Systems (AIS), 2011. Paper 80. Disponível em: http://aisel.aisnet.org/ecis2011/80. Acesso em: 17 jun. 2026.

KERBAJ, Richard. **The Secret History of the Five Eyes: The Untold Story of the International Spy Network**. London: Kings Road Publishing, 2022.

LIANG, Yikai *et al.* The effects of e-Government cloud assimilation on public value creation: An empirical study of China. **Government Information Quarterly**, v. 36, n. 4, p. 101397, 2019. DOI: 10.1016/j.giq.2019.101397.

MARGETTS, Helen; DUNLEAVY, Patrick. The second wave of digital-era governance: a quasi-paradigm for government on the Web. **Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences**, v. 371, n. 1987, p. 20120382, 2013. DOI: 10.1098/rsta.2012.0382.

MEIJER, Albert; ZOURIDIS, Stavros. E-Government is an institutional innovation. *In:* BEKKERS, Victor; VAN DUIVENBODEN, Hein; THAENS, Marcel (ed.). **Information and Communication Technology and Public Innovation: Assessing the ICT-Driven Modernization of Public Administration**. Amsterdam: IOS Press, 2006. v. 7. (Innovation and the Public Sector). p. 219–229.

MELL, Peter; GRANCE, Timothy. **The NIST Definition of Cloud Computing**. Gaithersburg, MD, set. 2011. p. 7. DOI: 10.6028/NIST.SP.800-145. Disponível em: https://doi.org/10.6028/NIST.SP.800-145. Acesso em: 17 jun. 2026.

MOLINA, André Luiz Bandeira; PINTO, Danielle Jacon Ayres; PORTELLA, Guilherme. **Soberania digital e segurança da informação: um marco para o Estado brasileiro**. JOTA, Opinião e Análise. 14 out. 2025. Disponível em: https://www.jota.info/opinion-and-analysis/articles/soberania-digital-e-seguranca-da-informacao-um-marco-para-o-estado-brasileiro. Acesso em: 8 maio 2026.

NOVA ZELÂNDIA. **New Zealand Government Information Security Classification System — Overview Table**. Wellington, 2025.

NOVA ZELÂNDIA. DEPARTMENT OF THE PRIME MINISTER AND CABINET. **Protective Security Requirements (PSR) Policy Framework: Security Governance (GOV)**. Wellington, out. 2025. Disponível em: https://www.protectivesecurity.govt.nz/assets/psr/GOV-policy.pdf. Acesso em: 26 abr. 2026.

NOVA ZELÂNDIA. NATIONAL CYBER SECURITY CENTRE; GOVERNMENT CHIEF DIGITAL OFFICER. **New Zealand Information Security Manual (NZISM). Version 3.9**. Wellington, abr. 2025. Disponível em: https://nzism.gcsb.govt.nz/. Acesso em: 11 abr. 2026.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **International Covenant on Civil and Political Rights**. New York: United Nations General Assembly, 16 dez. 1966. Adopted by General Assembly resolution 2200A (XXI); entered into force 23 March 1976. Disponível em: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights. Acesso em: 20 mar. 2026.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS. **American Convention on Human Rights**: Pact of San Jose, Costa Rica. Washington, DC: Organization of American States, 22 nov. 1969. Adopted at San Jose, Costa Rica; entry into force 18 July 1978, in accordance with Article 74(2). Disponível em: https://www.refworld.org/legal/agreements/oas/1969/en/89844. Acesso em: 20 mar. 2026.

PAPALEONIDAS, Kris. **Classified Information in Cloud Services — New Era of Cyber Security**. Jun. 2025. Master of Science in Technology Thesis — Master's Degree Programme in Information and Communication Technology (Cyber Security) – University of Turku (UTU) — Department of Computing, Faculty of Technology, Turku, Finlândia. Orientadores: Jouni Isoaho; Antti Hakkala. Disponível em: https://www.utupub.fi/server/api/core/bitstreams/5cf6a778-bc56-4514-bd64-fd4248748765/content. Acesso em: 28 mar. 2026.

PAPYSHEV, Gleb; YARIME, Masaru. The state's role in governing artificial intelligence: development, control, and promotion through national strategies. **Policy Design and Practice**, v. 6, n. 1, p. 79–102, 2023. DOI: 10.1080/25741292.2022.2162252.

PAQUETTE, Scott; JAEGER, Paul T.; WILSON, Susan C. Identifying the security risks associated with governmental use of cloud computing. **Government Information Quarterly**, v. 27, n. 3, p. 245–253, 2010. DOI: 10.1016/j.giq.2010.01.002.

POHLE, Julia; THIEL, Thorsten. Digital sovereignty. **Internet Policy Review**, v. 9, n. 4, 2020. DOI: 10.14763/2020.4.1532. Disponível em: https://doi.org/10.14763/2020.4.1532. Acesso em: 17 jun. 2026.

REINO UNIDO. CABINET OFFICE; GOVERNMENT SECURITY GROUP. **Government Security Classifications Policy (GSCP) 2023**. Londres, 2023. Disponível em: https://www.gov.uk/government/publications/government-security-classifications. Acesso em: 11 abr. 2026.

REINO UNIDO. NATIONAL CYBER SECURITY CENTRE. **Cloud security guidance: 14 cloud security principles**. Londres, 2021. Atualização contínua. Disponível em: https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles. Acesso em: 11 abr. 2026.

ROBERTS, Huw *et al.* Safeguarding European values with digital sovereignty: an analysis of statements and policies. **Journal of Cyber Policy**, v. 6, n. 3, 2021. DOI: 10.1080/23738871.2021.2003453.

ROGUSKI, Przemysław. Digital sovereignty and cloud storage: does international law protect governmental data stored abroad? **Forum Prawnicze**, v. 4, n. 88, p. 62–78, 2025. DOI: 10.32082/fp.4(88).2025.1334. Acesso em: 28 mar. 2026.

RUOHONEN, Jukka. The treachery of images in the digital sovereignty debate. **Minds and Machines**, v. 31, p. 439–456, 2021. DOI: 10.1007/s11023-021-09566-7. Acesso em: 28 mar. 2026.

SOLMS, Rossouw von; NIEKERK, Johan van. From information security to cyber security. **Computers & Security**, v. 38, p. 97–102, 2013. DOI: 10.1016/j.cose.2013.04.004.

UKEJE, Ndukwe; GUTIERREZ, Jairo; PETROVA, Krassie. Information security and privacy challenges of cloud computing for government adoption: a systematic review. **International Journal of Information Security**, v. 23, p. 1459–1475, 2024. DOI: 10.1007/s10207-023-00797-6. Acesso em: 28 mar. 2026.

UNIÃO EUROPEIA. **Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança em toda a União (NIS2)**. Bruxelas: União Europeia, 2022. Jornal Oficial da União Europeia: L 333, 27 dez. 2022, p. 80–152. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%5C%3A32022L2555. Acesso em: 11 abr. 2026.

UNIÃO EUROPEIA. AGÊNCIA DA UNIÃO EUROPEIA PARA A CIBERSEGURANÇA (ENISA). **EUCS — EU Cybersecurity Certification Scheme for Cloud Services: candidate scheme (rascunho)**. Atenas, mar. 2024. Disponível em:

https://www.enisa.europa.eu/publications/eucs-cloud-scheme. Acesso em: 11 abr. 2026.

UNIÃO EUROPEIA. COMISSÃO EUROPEIA. **Regulamento de Execução (UE) 2024/2690, de 17 de outubro de 2024, que estabelece regras de aplicação da Diretiva (UE) 2022/2555 no que respeita aos requisitos técnicos e metodológicos das medidas de gestão dos riscos de cibersegurança**. Bruxelas: Comissão Europeia, 2024. Jornal Oficial da União Europeia: série L, 18 out. 2024. Disponível em: https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj.

WIMMER, Miriam. Limites e possibilidades para o uso secundário de dados pessoais no poder público: lições da pandemia. **Revista Brasileira de Políticas Públicas**, UniCEUB, Brasília, v. 11, n. 1, p. 122–142, 2021. ISSN 2236-1677. DOI: 10.5102/rbpp.v11i1.7136.

YOUSUF, Shoaib *et al.* **Sovereign Clouds Are Reshaping National Data Security**. Boston, MA: Boston Consulting Group, jun. 2025. Boston Consulting Group (BCG). Publicado em: 27 jun. 2025. Disponível em: https://web-assets.bcg.com/pdf-src/prod-live/sovereign-clouds-reshaping-national-data-security.pdf. Acesso em: 11 abr. 2026.

ZWEIGERT, Konrad; KÖTZ, Hein. **An Introduction to Comparative Law**. Tradução: Tony Weir. 3. ed. Oxford: Oxford University Press, 1998.

Apêndice A Pedidos de acesso à informação (LAI)

Tabela 2. Pedidos de acesso à informação realizados

Órgão / NUP	Pedido / Resposta	Objeto	Síntese da resposta	Dec.
GSI/PR 00137.002849/2026-10	24/03-24/04	Implementação da IN 8/2025: habilitações (art. 8.º) e orientações complementares; NC09 e algoritmos registrados.	nenhum provedor habilitado pelo GSI/PR na forma do art. 8.º da IN 8/2025; GSI/PR não tem informações sobre habilitação por órgãos de registro nível 1. Nenhum algoritmo registrado nos termos da NC09. Guia técnico de recursos criptográficos previsto na NC09 não elaborado e sem previsão; NC09 em revisão. Nota técnica que fundamentou a edição da IN 8/2025 anexada.	Concedido
SGD/MGI 18002.003987/2026-15	25/03-28/04	Maturidade do SISP em segurança da informação, contratos de nuvem de governo e orientação complementar sobre tratamento de informações classificadas em nuvem.	Negados os resultados agregados de maturidade (indicadores iBase/iSeg) e o número de instituições com contratos. Tratamento de informações classificadas em nuvem "em discussão com a CGU", sem definição formal sobre publicação de orientação complementar.	Parc. concedido
Serpro 18870.000928/2026-58	24/03-08/04	Capacidade técnica para o cumprimento da IN 8/2025: certificações ISO/IEC, habilitação e criptografia. Número de contratos de nuvem.	ISO/IEC 27001 e 27701 para alguns produtos e serviços; 27017 e 27018 em planejamento. Não habilitado nem em processo (sem impedimento técnico, ausente demanda institucional), porém em condições de tratar informações classificadas em infraestrutura local. Criptografia de Estado não atendida; "algoritmos criptográficos de Estado possuem uso restrito e não são amplamente disponibilizados [...] não estando atualmente sob posse ou gestão do Serpro". 17 órgãos/entidades mantêm contratos de nuvem de governo.	Concedido
Dataprev 36783.010932/2026-95	24/03-09/04	Capacidade técnica para o cumprimento da IN 8/2025: certificações ISO/IEC, habilitação e criptografia. Número de contratos de nuvem.	ISO/IEC 27001:2022 para *data center*; emissor Fundação Vanzolini; validade 08/01/2029. Não habilitada nem em processo; Negados detalhes sobre cumprimento dos requisitos do art. 3.º da IN. 4 instituições mantêm contratos de nuvem. Não oferece custódia de chaves com algoritmo de Estado.	Parc. concedido
Telebras 00132.000048/2026-60 (negado) 00132.000075/2026-32 (com recurso)	25/03-24/04 10/05-10/06 11/06-19/06 (recurso)	Capacidade técnica para o cumprimento da IN 8/2025: certificações ISO/IEC, habilitação e criptografia. Número de contratos de nuvem.	Negados o acesso às certificações, os detalhes sobre o cumprimento de requisitos e o número de contratos de nuvem. Em processo de habilitação como órgão de registro nível 2.	Parc. concedido (em recurso)

Fonte: Elaborada pelo autor (2026).

Apêndice B Regras de codificação da matriz comparativa

Este apêndice documenta as regras de decisão aplicadas na codificação da matriz comparativa (Tabela 1), em atenção à reprodutibilidade da análise.

(i) **Objeto da avaliação.** A codificação incide sobre a previsão normativa. "Especificação técnica suficiente" é entendida como a presença de parâmetros operacionais para o cumprimento do critério: elementos objetivos, limiares ou padrões técnicos referenciados, órgão responsável identificado e, quando aplicável, periodicidade definida.

(ii) **Nível de sensibilidade de referência.** A célula reflete a previsão no nível de sensibilidade mais alto que a jurisdição autoriza publicamente em nuvem. Para jurisdições que vedam o tratamento de informação classificada em nuvem (p. ex. Nova Zelândia), a avaliação considera o regime no teto autorizado.

(iii) **Fontes.** A codificação baseia-se em fontes primárias vigentes na data da coleta, incluídas as remissões a outros instrumentos.

(iv) **Regra de desempate.** Quando a evidência se situa entre dois níveis, adota-se o nível inferior (critério conservador), registrando-se a justificativa na legenda da matriz. A ausência de menção de existência em fonte pública verificável é codificada como $\times$.

(v) **Triangulação de fontes.** Cada codificação foi sustentada pela convergência de, no mínimo, duas fontes de natureza distinta (norma e documento técnico, ou norma e literatura secundária). Trata-se de triangulação de dados, que mitiga possível erro por fonte única (Denzin, 2009; Bowen, 2009).

Tabela 3. Regras de decisão para a codificação dos critérios (✓ atende; ○ parcial; × não atende)

Critério	✓ — Atende	○ — Parcial	× — Não atende
Grupo A — Estrutural			
A1 Escopo por grau de sigilo e modelo de serviço	Define os graus tratáveis em nuvem e diferencia por modelo de serviço (IaaS/PaaS/SaaS) e/ou implantação.	Delimita apenas parcialmente (graus ou modelos, não ambos; mapeamento incompleto ou ambíguo).	Inexiste regra de escopo por grau de sigilo.
A2 Habilitação/certificação de provedores	Processo com critérios definidos, avaliador independente/acreditado, periodicidade e, idealmente, catálogo público de provedores.	Processo com lacunas (sem periodicidade, sem lista pública, avaliador não independente).	Inexiste processo definido.
A3 Responsabilidade compartilhada	Modelo explícito, diferenciado por modelo de serviço, com obrigações documentadas para ambas as partes (p. ex. cláusulas-modelo).	Princípio enunciado, sem especificação ou operacionalização da divisão.	Inexiste previsão de responsabilidade compartilhada.
A4 Soberania jurisdicional e imunidade a legislação estrangeira	Proteção explícita: obrigação de prever imunidade jurídica a lei extraterritorial, limites de controle societário estrangeiro, ou vedação de provedor sob jurisdição de terceiros.	Proteção parcial/indireta: residência de dados ou avaliação de controle estrangeiro, ou estabelecimento nacional e infraestrutura dedicada, sem vedar provedor sujeito a lei extraterritorial.	Inexiste previsão de proteção.

continua...

Tabela 3. (continuação)

Critério	✓ — Atende	○ — Parcial	× — Não atende
A5 Credenciamento e verificação de pessoas	Credenciamento exigido e especificado (níveis, profundidade da verificação), ainda que por remissão a regime detalhado.	Triagem mencionada sem especificação suficiente.	Inexiste requisito sobre pessoas.
Grupo B — Técnico-operacional			
B1 Gerenciamento de chaves criptográficas	Gestão exigida com especificação técnica do ciclo de vida das chaves (componentes mínimos de geração, custódia, rotação, revogação e destruição), cumulada com ao menos um mecanismo técnico vinculante: custódia pelo contratante com exigência de *hardware security module* (HSM) ou restrição a algoritmos aprovados.	Controle das chaves pelo contratante e/ou algoritmos aprovados exigidos, sem especificação dos componentes do ciclo de vida.	Inexiste previsão de gestão de chaves.
B2 Localização de dados e estratégia de saída	Residência de dados *e* estratégia de saída/apagamento seguro exigidas e especificadas.	Apenas um dos requisitos presente, ou presente sem especificação suficiente.	Inexistem ambos os requisitos.
B3 Auditoria independente e monitoramento contínuo	Auditoria por terceiro independente vinculada a esquema de certificação acreditado e específico para nuvem, com periodicidade definida, somada a monitoramento contínuo e notificação de incidentes.	Monitoramento/*logging* exigido, mas auditoria não independente ou sem periodicidade fixada.	Inexistem auditoria independente e monitoramento contínuo.
B4 Segurança da cadeia de suprimentos de TIC	Regime dedicado, com controles sobre fornecedores e subcontratados (família de controles específica, avaliação de influência estrangeira ou processo de gestão de riscos na cadeia de suprimentos estruturado).	Tratada no âmbito de controles gerais, sem regime dedicado, ou apenas por via contratual.	Inexiste previsão de segurança da cadeia de suprimentos.

Apêndice C Requisitos de segurança da informação do quadro normativo brasileiro

Este apêndice compila os requisitos de segurança da informação aplicáveis ao tratamento de informações classificadas em computação em nuvem pelo Poder Executivo federal, conforme o quadro normativo brasileiro examinado. Os requisitos estão organizados em cinco blocos funcionais e remetem aos instrumentos normativos de origem. A síntese discursiva correspondente encontra-se na seção 5.1.

Tabela 4. Requisitos para tratamento de informações classificadas em nuvem no Poder Executivo federal brasileiro

Tipo	Previsão	Instrumento	C.
I — Requisitos estruturais			
Tipo de nuvem	Admite exclusivamente nuvem privada ou comunitária gerida por órgão de registro ou posto de controle habilitado para *reservado* e *secreto*; *ultrassecreto* vedado em qualquer modelo de nuvem	IN GSI/PR n.º 8/2025, arts. 2.º e 6.º	A1
Classificação prévia da informação	Classificação prévia das informações nos termos do Decreto n.º 7.724/2012 antes da definição do modelo de nuvem a ser contratado	Portaria SGD/MGI n.º 5.950/2023, Anexo I, item 5.3; IN GSI/PR n.º 5/2021, art. 11, caput, V	A1
Planejamento prévio e gestão de riscos	Antes da transferência: alinhamento à legislação (privacidade, proteção de dados pessoais, sigilo); gestão de riscos com relatório de impacto; avaliação do tipo de informação, fluxo e valor dos ativos; definição do modelo de serviço e de implantação; sistemas estruturantes somente em nuvem privada ou comunitária; planejamento de custos de migração	IN GSI/PR n.º 5/2021, art. 11, caput, I a VII	A1
Habilitação do provedor	Provedor deve ser habilitado como órgão de registro ou posto de controle	IN GSI/PR n.º 8/2025, art. 8.º; Decreto n.º 7.845/2012, arts. 10 e 11	A2
II — Requisitos do ambiente			
Segmentação e isolamento	Segmentação de rede; isolamento entre máquinas virtuais e de contêineres; proteção contra usuários externos e segregação lógica de dados, aplicações, sistemas operacionais, armazenamento e rede; separação dos recursos do provedor	IN GSI/PR n.º 8/2025, art. 3.º, caput, I, II e III; IN GSI/PR n.º 5/2021, art. 15, caput, I a IV	—
Criptografia de Estado	Cifração de todas as informações classificadas em repouso e em trânsito com recurso criptográfico baseado em algoritmo de Estado; parâmetros definidos pelo GSI/PR	IN GSI/PR n.º 8/2025, art. 3.º, caput, IV; Decreto n.º 7.845/2012, art. 40; IN GSI/PR n.º 3/2013; NC09/IN01/DSIC/GSIPR/2014	B1
Gerenciamento de chaves criptográficas	Chaves gerenciadas exclusivamente pelos órgãos de registro e não armazenadas na nuvem; políticas e procedimentos de gerenciamento de chaves observados por cliente e provedor, com esquema criptográfico adequado ao nível de sigilo; uso, *sempre que possível*, de chaves baseadas em *hardware*	IN GSI/PR n.º 8/2025, art. 3.º, caput, V; Portaria SGD/MGI n.º 5.950/2023, Anexo I, item 10.2, alíneas *j* e *k*; IN GSI/PR n.º 5/2021, art. 14, caput, III, e art. 20, caput, VIII e IX	B1
Governança de recursos criptográficos	Recursos criptográficos sob o mesmo regime das informações classificadas: inventário, vistorias periódicas e notificação de anormalidades à autoridade competente	Decreto n.º 7.845/2012, art. 41; IN GSI/PR n.º 3/2013	B1
Backup e recuperação	*Backups* criptografados em infraestrutura local, com garantia de recuperação em caso de desastre	IN GSI/PR n.º 8/2025, art. 3.º, caput, VI	B2
Autenticação e gestão de identidades	Autenticação multifatorial; certificado digital como mecanismo mínimo; identidade federada e *single sign-on*; negação de acesso direto do provedor ao ambiente de autenticação	IN GSI/PR n.º 8/2025, art. 3.º, caput, VII; Decreto n.º 7.845/2012, art. 38, § 2.º; IN GSI/PR n.º 5/2021, art. 13, caput, I a III	—

continua...

Tabela 4. (continuação)

Tipo	Previsão	Instrumento	C.
Controle de acesso	Acesso restrito a pessoas credenciadas com necessidade de conhecer; RBAC/ABAC com revisão mínima semestral; gestão centralizada de identidades e ciclo de vida de acessos	IN GSI/PR n.º 8/2025, art. 3.º, caput, VIII, XI e XII; Decreto n.º 7.845/2012, art. 38, § 3.º	—
Monitoramento de atividades suspeitas	Mecanismos automatizados de alertas para atividades suspeitas	IN GSI/PR n.º 8/2025, art. 3.º, caput, X	B3
Retenção de registros	Registros detalhados e imutáveis de todos os acessos, com auditorias periódicas por equipe independente; retenção igual ou superior à da restrição de acesso (mínimo de cinco anos no provedor ou em ambiente próprio controlado)	IN GSI/PR n.º 8/2025, art. 3.º, caput, IX; Decreto n.º 7.845/2012, art. 38, § 4.º; Portaria SGD/MGI n.º 5.950/2023, Anexo I, item 10.2, alíneas *f* e *g*; IN GSI/PR n.º 5/2021, art. 13, caput, IV a VII	B3
Vedação de acesso do provedor ao conteúdo	Controles técnicos e administrativos que impeçam o acesso do provedor ao conteúdo das informações classificadas	IN GSI/PR n.º 8/2025, art. 3.º, caput, XIII	A4
Isolamento de dispositivos de produção	Equipamentos e sistemas para produção de documentos classificados física ou logicamente isolados, com recursos criptográficos adequados	Decreto n.º 7.845/2012, art. 39	—
III — Requisitos do provedor			
Estabelecimento e infraestrutura	Estabelecido no Brasil; recursos físicos em *data centers* em território nacional; infraestrutura física dedicada; alta disponibilidade com redundância e planos de recuperação de desastres	IN GSI/PR n.º 8/2025, art. 7.º, caput, I, III, IV e V	A4
Certificações de segurança	Certificações ISO/IEC vigentes: ABNT NBR ISO/IEC 27001, 27017, 27018, 27701 e 22237	IN GSI/PR n.º 8/2025, art. 7.º, caput, II, alíneas *a* a *e*	A2
Requisitos técnicos do provedor	Metodologia de gestão de riscos; fortalecimento da virtualização; segurança de aplicações *web* (testes de penetração; correção de vulnerabilidades); continuidade e recuperação de desastres; canal seguro (SSL/TLS); segregação de dados; descarte seguro de ativos	IN GSI/PR n.º 5/2021, art. 20, caput, I a VII, X e XI	—
Proteção contra ameaças avançadas	Mecanismos de proteção contra ameaças persistentes avançadas (APT) e acessos não autorizados	IN GSI/PR n.º 8/2025, art. 7.º, caput, VI	—
Credenciamento de pessoas (provedor)	Providenciar, junto ao órgão de registro contratante, o credenciamento de segurança de pessoas físicas com acesso à infraestrutura	IN GSI/PR n.º 8/2025, art. 7.º, caput, VIII; Decreto n.º 7.845/2012; IN GSI/PR n.º 10/2026	A5
Conformidade, cooperação e preservação de evidências	Garantir conformidade com as normas e padrões; cooperar com autoridades em investigações; notificar imediatamente incidentes; preservar e entregar indícios e evidências	IN GSI/PR n.º 8/2025, art. 10, caput, I, III e IV; IN GSI/PR n.º 5/2021, art. 20, caput, XII e XIII	B3
Relatório anual de segurança	Fornecer ao órgão contratante relatório anual sobre segurança das informações classificadas (segurança cibernética, de rede, de nuvem, de aplicações e de dados)	IN GSI/PR n.º 8/2025, art. 10, caput, II	B3
Auditoria independente (SOC 2)	Demonstrar conformidade com os padrões de segurança de nuvem por meio de auditoria anual SOC 2 conduzida por auditor independente, com apresentação dos relatórios tipo I e tipo II	IN GSI/PR n.º 5/2021, art. 20, caput, XIV	B3
Restrição de acesso às instalações	Impedir que pessoas não autorizadas pelo órgão contratante tenham acesso aos recursos e instalações onde estão armazenadas as informações	IN GSI/PR n.º 8/2025, art. 10, caput, V	—
IV — Responsabilidades do órgão contratante			
Contrato sigiloso	Estabelecer contrato sigiloso, com previsão expressa de observância da IN 8/2025 pela contratada	IN GSI/PR n.º 8/2025, art. 9.º, caput, I; Decreto n.º 7.845/2012, art. 48	A3

continua...

Tabela 4. (continuação)

Tipo	Previsão	Instrumento	C.
Cláusulas de confidencialidade, de propriedade e de uso	Celebrar termo de confidencialidade vedando transferência a empresas e governos estrangeiros; direitos exclusivos de propriedade do órgão sobre dados, cópias e *logs*; proibição de uso secundário (propaganda, IA); conformidade da política do provedor com a lei brasileira	IN GSI/PR n.º 5/2021, art. 19, caput, I a IV; Portaria SGD/MGI n.º 5.950/2023, Anexo I, item 10.2, alíneas *e* e *n*	A4
Auditoria do provedor	Auditoria técnica do órgão contratante sobre o cumprimento dos requisitos; monitorar e auditar, no mínimo anualmente, com escopo técnico mínimo, periodicidade e critérios de conformidade previamente definidos	IN GSI/PR n.º 8/2025, art. 7.º, parágrafo único, e art. 9.º, caput, II	B3
Gestão da nuvem e matriz de responsabilidades	Documentação, pelo provedor, de papéis e responsabilidades de SI; elaboração de matriz de responsabilidades; processo conjunto de tratamento de incidentes	IN GSI/PR n.º 5/2021, art. 16, caput, II a IV; Portaria SGD/MGI n.º 5.950/2023, Anexo I, item 25 e Anexo IV	A3
Atualizações e revisão de riscos	Definição de critérios e periodicidade das atualizações do provedor; revisão periódica dos processos internos de gestão de riscos	IN GSI/PR n.º 5/2021, art. 12, caput, I e II	—
Credenciamento de pessoas (órgão)	Realizar o credenciamento de segurança de todas as pessoas que acessem e operem a infraestrutura de nuvem classificada	IN GSI/PR n.º 8/2025, art. 9.º, caput, III; Decreto n.º 7.845/2012; IN GSI/PR n.º 10/2026	A5
Capacitação	Capacitar periodicamente equipe com acesso a informações classificadas em proteção de dados, segurança da informação e incidentes cibernéticos	IN GSI/PR n.º 8/2025, art. 9.º, caput, IV; IN GSI/PR n.º 5/2021, art. 16, caput, I	A5
Apuração e resposta a incidentes	Apurar eventual infração em caso de suspeita de descumprimento; adotar imediatamente as ações necessárias em caso de suspeita de comprometimento, inclusive a suspensão do acesso	IN GSI/PR n.º 8/2025, art. 9.º, caput, V e VI	B3
V — Localização de dados e estratégia de saída			
Armazenamento em território nacional	Armazenamento e processamento exclusivamente em *data centers* em território nacional; vedação de replicação ou *backup* fora do país	IN GSI/PR n.º 8/2025, art. 5.º, caput e parágrafo único	B2
Localização e cópias de segurança (regime geral)	Hospedagem em território brasileiro; ao menos uma cópia de segurança em território nacional; vedação de tratamento fora do país para informação com restrição de acesso; observância da LGPD	IN GSI/PR n.º 5/2021, art. 18, caput, I a IV; Portaria SGD/MGI n.º 5.950/2023, Anexo I, item 5.4.5	B2
Trânsito em redes nacionais	Trânsito em redes exclusivamente em território nacional; exceção para comunicações diplomáticas e missões oficiais, mediante criptografia compatível e autorização da alta administração	IN GSI/PR n.º 8/2025, art. 4.º, caput, e § 1.º, I e II	B2
Portabilidade e reversibilidade	Portabilidade de dados e aplicativos sem custo adicional; encerramento contratual com devolução integral e eliminação segura dos dados; direito ao esquecimento para dados pessoais	Portaria SGD/MGI n.º 5.950/2023, Anexo I, itens 8.5 e 24.1; IN GSI/PR n.º 5/2021, art. 19, caput, V a VII	B2

Notas: a coluna "C." remete aos critérios da matriz comparativa (Grupo A: A1–A5; Grupo B: B1–B4). Os requisitos do art. 3.º da IN GSI/PR n.º 8/2025 não são expressamente atribuídos ao órgão contratante ou ao provedor. Os requisitos da Portaria SGD/MGI n.º 5.950/2023 aplicam-se somente aos órgãos e entidades do SISP.
Fonte: Elaborada pelo autor (2026).

Apêndice D Síntese dos referenciais selecionados

Tabela 5. Síntese dos referenciais selecionados

País/ Bloco	Instrumentos	Informações classificadas em nuvem	Detalhamento dos requisitos
EUA	*Federal Risk and Authorization Management Program* (FedRAMP), nos níveis *Low*, *Moderate* e *High*; *Committee on National Security Systems Instruction No. 1253* (CNSSI 1253); *Department of Defense Cloud Computing Security Requirements Guide* (DoD CC SRG), no *Impact Level 6* (IL6), para dados secretos; *Security and Privacy Controls for Information Systems and Organizations* (NIST SP 800-53 Rev. 5.2.0) (EUA, 2026, 2014, 2025)	*Secret* (IL6) exigem FedRAMP High acrescido de controles para sistemas de segurança nacional (CNSSI 1253 + *Classified Information Overlay*), uso da rede segregada SIPRNet e instalações classificadas; dados *Top Secret*/SCI admitem tratamento em nuvem comunitária da comunidade de inteligência (IC Cloud), com controles adicionais e infraestrutura certificada TS/SCI conectada à rede segregada JWICS. Nuvem comercial padrão não autorizada para dados classificados.	**Autorização de operação**: emitida pelo órgão federal contratante (*agency* ATO), após avaliação por organização de avaliação de terceira parte acreditada pelo governo federal (3PAO); catálogo público de provedores autorizados (*FedRAMP Marketplace*, 300+ autorizações); presunção legal de adequação para agências federais (*FedRAMP Authorization Act*). **FedRAMP High**: 410 controles do NIST SP 800-53; monitoramento contínuo com relatórios mensais de vulnerabilidades e avaliação anual de controles por 3PAO. **Segurança da cadeia de suprimentos**: família SR (12 controles) do NIST SP 800-53 Rev. 5.2.0, incluindo avaliação de fornecedores de hardware e software (SR-3, SR-5 e SR-11). **Gestão de chaves**: órgão deve manter controle das chaves-mestras; NIST SP 800-144 estabelece que o órgão deve controlar o material de chaves central
Austrália	*Information Security Manual* (ISM, edição mar. 2026), publicado pela *Australian Signals Directorate* (ASD); *Protective Security Policy Framework* (PSPF 2025, Dep. do Interior); *Infosec Registered Assessors Program* (IRAP) (Austrália, 2026, 2025a, 2020, 2025b)	*Secret* e *Top Secret*: admitidos apenas em nuvens comunitárias ou privadas, conforme controle ISM-1529; dados *Top Secret* requerem avaliação conduzida pela própria ASD. O PSPF 2025 nomeia explicitamente os riscos de provedores estrangeiros: sujeição a controle extrajudicial por entidade estrangeira, possibilidade de divulgação compulsória de dados e impacto nos níveis de segurança de pessoas contratadas pelo provedor. Req. 0046 exige avaliação de controle ou influência estrangeira (FOCI) sobre provedores	**IRAP obrigatório** para toda nuvem que processe dados classificados: avaliação técnica por assessor credenciado pela ASD (não pelo próprio órgão); periodicidade máxima de 24 meses (Req. 0109 do PSPF). **Qualificações do assessor IRAP**: CISSP ou CISM ou GSLC; CISA ou QSA ou ISO 27001 Lead Auditor; 5 anos de experiência em TI; aprovação em exame ASD. **Hosting Certification Framework (HCF)**: dados OFFICIAL: Sensitive e classificados devem ser hospedados em provedores certificados pelo HCF (Req. 0111, vigência jul. 2025). **Criptografia pós-quântica**: algoritmos PQC aprovados exigidos em todos os novos equipamentos e software criptográficos (Req. 0212, PSPF 2025). **Credenciamento de pessoas**: conduzido de forma centralizada pela Australian Government Security Vetting Agency - AGSVA
Reino Unido	*Government Security Classifications Policy* (GSCP 2023, Cabinet Office); *Cloud security guidance: 14 cloud security principles*, do *National Cyber Security Centre* (NCSC) (Reino Unido, 2023, 2021)	*Secret*: vedado em nuvem pública; criptografia aprovada pelo NCSC obrigatória na transmissão; MFA obrigatório e credenciamento de segurança nacional (NSV) para acesso; orientações técnicas complementares classificadas; plano estratégico do Ministério da Defesa (MoD) para uso de *Secret* em nuvem privada dedicada (MODCloud) em execução. *OFFICIAL* (incluindo *OFFICIAL-SENSITIVE*): política *Cloud First*: nuvem é a opção padrão; nuvem pública amplamente adotada com avaliação pelos 14 princípios do NCSC	**14 princípios NCSC**: avaliação de provedores com base em proteção de dados em trânsito; proteção de ativos; separação entre contratantes; governança; segurança operacional; segurança de pessoas; desenvolvimento seguro; segurança da cadeia de suprimentos (princípio 8); gestão de identidade e autenticação; e proteção de interfaces. **Segurança de pessoas**: provedores que processam informação classificada devem obter credenciamento de segurança e submeter pessoas a verificações de antecedentes proporcionais ao nível de acesso; aplicam-se controles de cadeia de suprimentos a subcontratados (GSCP, seção 1.6). **Cadeia de suprimentos**: cadeia de suprimentos do provedor deve atender aos mesmos padrões de segurança do contratante

continua...

Tabela 5. (continuação)

País/ Bloco	Instrumentos	Informações classificadas em nuvem	Detalhamento dos requisitos
França	*Référentiel d'exigences SecNumCloud* (SecNumCloud v3.2, ANSSI); *Instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale* (IGI 1300); *Instruction interministérielle n° 901 relative à la protection des systèmes d'information sensibles et Diffusion Restreinte* (II 901) (França, 2022, 2021, 2024)	Inviabilizado estruturalmente para *Secret* e *Très Secret*: regras de separação física (CLOIS_01), de vedação de acesso remoto (NOMAD_08) e de exigência de dispositivos aprovados pela ANSSI (DISP_SEC_01) da IGI 1300 são incompatíveis com qualquer modelo de nuvem; nuvem qualificada pelo SecNumCloud admitida, com requisitos cumulativos adicionais, para *Diffusion Restreinte* (menção de proteção administrativa abaixo do nível classificado, sem equivalente direto no quadro brasileiro)	**Qualificação ANSSI**: avaliação por laboratório de avaliação acreditado (CESTI), em quatro etapas progressivas (jalons J0–J3); 263 exigências em 19 capítulos; reavaliação por mudança relevante e periodicamente. **Para DR**: SecNumCloud; homologação do sistema pelo órgão (II 901, art. 13); cifração obrigatória com meios aprovados pela ANSSI fora de zona fisicamente protegida (II 901, art. 14); prestação preferencialmente a partir do território nacional e atenção à nacionalidade dos administradores do provedor (Recomendações ANSSI, jul. 2024). **Requisitos de soberania jurisdicional** (exigência 19.6): sede do provedor na UE; capital extra-UE limitado a 24% individualmente e 39% coletivamente; vedação técnica de acesso por entidades extra-UE. **Outros requisitos**: cifração com chave por contratante (exigência 10.1); proteção de chaves de administração por módulo de segurança de hardware (exigência 10.5); dados e administração exclusivamente em território da UE (exigência 19.2); apagamento seguro com pré-aviso de 21 dias (exigência 19.4)
União Europeia	*European Cybersecurity Certification Scheme for Cloud Services* (EUCS, ENISA, rascunho 2024); *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union* (NIS2); *Cybersecurity Act* (EUCSA, Regulamento (UE) 2019/881) (União Europeia, 2024a, 2022)	Nível *High* do EUCS (equivalente funcional a dados sensíveis de alto impacto): avaliação independente e auditoria periódica; os rascunhos de 2020–2023 exigiam imunidade técnica e jurídica a legislação extraterritorial, requisito removido do rascunho de 2024 e substituído pela *International Company Profile Attestation* (ICPA); o debate político sobre o requisito de soberania permanece em aberto na Comissão Europeia	**Certificação por organismo de avaliação da conformidade (CAB)**: credenciado pela autoridade nacional de supervisão de cibersegurança; três níveis de garantia: *Basic* (autodeclaração), *Substantial* (revisão de terceiros) e *High* (auditoria independente rigorosa). **Obrigatoriedade**: certificação voluntária; o art. 21.3 da NIS2 faculta aos Estados-membros exigir o uso de serviços de nuvem certificados, convertendo-a em obrigação setorial *de facto*. **Segurança da cadeia de suprimentos**: art. 21.2(d) da NIS2 exige gestão de riscos da cadeia de suprimentos, incluindo fornecedores diretos de hardware e software. **Requisitos de soberania**: debate sobre exclusão de provedores extra-UE ainda em aberto; rascunho 2024: ICPA (declaração de jurisdições verificada), sem vedação de capital extra-UE. **Gestão de chaves**: requisito de controle das chaves criptográficas pelo contratante no nível High do EUCS. **NIS2, art. 21**: medidas de segurança incluem gestão de incidentes, continuidade de negócios, segurança da cadeia de suprimentos, segurança de redes e sistemas, políticas de criptografia, MFA e comunicações seguras
Nova Zelândia	*New Zealand Information Security Manual* (NZISM v3.9, abr. 2025), publicado pelo *National Cyber Security Centre* (NCSC-NZ); *Protective Security Requirements* (PSR v1.0, out. 2025, DPMC), incluindo *Information Security* (INFOSEC) e *Supply Chain Security* (GOV 5) (Nova Zelândia, 2025c,a,b)	Vedação para *Confidential*, *Secret* e *Top Secret* em nuvem pública, híbrida ou operada por provedor externo à agência (CID:4802 e CID:7388 — *Must Not*): proibição sem exceção admissível; apenas infraestrutura própria da agência. Vedação extensiva a informações com marcação *New Zealand Eyes Only* (NZEO) (CID:4803 e CID:7389)	**Acreditação formal**: pelo *Accreditation Authority* (GCSB/NCSC-NZ); os sistemas são acreditados por nível de classificação antes da entrada em serviço. **Avaliações de garantia periódicas**: por avaliadores qualificados independentes (CID:7397 — *Should*). **Gerenciamento de chaves**: plano de gerenciamento de chaves (KMP) obrigatório antes de armazenar dados na nuvem, cobrindo diferenças específicas do ambiente de nuvem (CID:7462 — *Must*); módulo de segurança de hardware (HSM) necessário para chaves de alto valor (seção 17.10 do NZISM). **Estratégia de saída**: obrigatória para cada serviço de nuvem, incluindo processo de recuperação e apagamento de dados ao término do contrato (CID:7511–7513 — *Must*). **Logging**: *logs* coletados pelo provedor devem ser incorporados aos sistemas corporativos de forma tempestiva (CID:7498 —*Must*); *logs* com integridade verificável (CID:7496). **Cadeia de suprimentos** (GOV 5, PSR): 12 princípios para gestão de risco de fornecedores, com requisitos de segurança em contratos e atividades de assurance ao longo do ciclo de vida contratual

continua...

Tabela 5. (continuação)

País/ Bloco	Instrumentos	Informações classificadas em nuvem	Detalhamento dos requisitos
Canadá	*Policy on Government Security* (TBS, atual. 2025) e *Directive on Security Management* e *Directive on Security Screening* (2025); *Directive on Service and Digital* (atual. out. 2025); *Direction for Electronic Data Residency* (ITPIN 2017-02); *Secure Use of Commercial Cloud Services* (SPIN 2017-01, atual. out. 2025); *GC Cloud Guardrails* (13 *guardrails*, atual. 2024); *GC Cloud Security Risk Management Approach and Procedures* (TBS, 2018); *IT Security Risk Management: A Lifecycle Approach* (ITSG-33, CCCS/CSE); *White Paper: Data Sovereignty and the Public Cloud* (TBS, 2018); *Digital Sovereignty Framework* (nov. 2025); *Direction on Post-Quantum Cryptography Migration* (SPIN, out. 2025) e *Preparing Your Organization for the Quantum Threat to Cryptography* (ITSM.40.001, Cyber Centre, 2025) (Canadá, 2019b,a, 2025c,e, 2017a,b, 2024, 2018a, 2012, 2018b, 2025b,d,a)	Teto de *Protected B* para nuvem comercial; residência de dados no Canadá obrigatória para *Protected B/C* e *Classified*; sistemas *classified* remetidos à orientação do Cyber Centre, sem parâmetros publicizados.	**Autorização de operação (ATO)**: emitida pelo órgão, conforme a *GC Cloud Security Risk Management Approach and Procedures* (TBS, 2018), com apoio do CCCS/CSE e referência de controles do ITSG-33 (equivalente funcional do NIST SP 800-37). **GC Cloud Guardrails**: 13 controles mínimos obrigatórios nos primeiros 30 dias úteis de uso de qualquer serviço de nuvem, incluindo localização geográfica no Canadá (G5), criptografia em trânsito e em repouso (G6–G7) e *logging*/auditabilidade (G11). **Estratégia de saída**: obrigatória nos contratos (*GC Cloud Adoption Strategy*). **Credenciamento de pessoas**: *Directive on Security Screening* (níveis *Reliability Status*, *Secret* e *Top Secret*; *Top Secret* exige cidadania canadense). **Soberania de dados**: o teto de *Protected B* para nuvem comercial é decisão de soberania fundamentada no risco do CLOUD Act / PATRIOT Act / FISA (*White Paper*, 2018). **Criptografia pós-quântica (PQC)**: migração obrigatória para PQC dos sistemas até *Protected B* (SPIN, out. 2025; *roadmap* ITSM.40.001), com prazos de 2031 (alta prioridade) e 2035 (demais) e cláusulas de PQC/CMVP em contratos; sistemas *classified* remetidos ao Cyber Centre. **Soberania operacional**: o Digital Sovereignty Framework (nov. 2025) define controles de *procurement*, de suprimento e técnicos, igualmente restritos a *Protected B* e abaixo

Fonte: Elaborada pelo autor (2026).