# Ecossistema de Comunicações Soberano Brasileiro

**Vinícius Lagrota**[1], **Rodrigo Pacheco**[1], **Matheus Engel**[1], **Vanderson Rocha**[1]

[1] Research and Development Center for Communication Security (CEPESC)
Brasília, DF – Brazil.

vinicius.lagrota@gmail.com, rppacheco.85@gmail.com,
matheus_spe@poli.ufrj.br, somrocha@gmail.com

***Abstract.*** *Este artigo discute a soberania digital estatal como requisito estratégico para a proteção de dados, ativos estratégicos, infraestruturas críticas e comunicações sensíveis. Apresenta-se um ecossistema soberano de comunicações brasileiro, estruturado em torno de uma ICP soberana, bibliotecas criptográficas, sistemas operacionais hardenizados, aplicações seguras e plataformas de hardware nacionais. O ecossistema integra identidade digital, custódia de chaves, criptografia de Estado e mecanismos pós-quânticos em diferentes cenários de uso. O ecossistema busca reduzir dependências tecnológicas e jurisdicionais externas, fortalecendo a autonomia, a segurança e o controle institucional do Estado brasileiro sobre ativos estratégicos de informação.*

## 1. Introdução

A transformação digital ampliou a dependência do Estado de infraestruturas computacionais e canais eletrônicos para conduzir políticas públicas, custodiar informações sensíveis e coordenar funções críticas de governo. Nesse cenário, comunicações seguras tornam-se essenciais para garantir a capacidade estatal de preservar confidencialidade, integridade, disponibilidade e autenticidade em processos administrativos, diplomáticos, militares e de inteligência.

Essa dependência ocorre em um ambiente marcado por cadeias tecnológicas globais, concentração de plataformas e assimetrias jurisdicionais. Quando aplicações, nuvens, componentes de software ou mecanismos criptográficos estratégicos permanecem subordinados a provedores, padrões ou marcos legais estrangeiros, o Estado se expõe a riscos de dependência, descontinuidade, indisponibilidade e acesso extraterritorial a dados. Assim, a dimensão tecnológica passa a integrar diretamente a agenda de soberania estatal [União Europeia 2016, Congressional Research Service 2018, Commission Nationale de l'Informatique et des Libertés 2024].

A evolução da computação quântica intensifica esse desafio. Os algoritmos de Shor e Grover indicam que parte das bases criptográficas atualmente empregadas pode ser afetada por avanços nesse campo [Shor 1997, Grover 1996]. Em resposta, países vêm estruturando estratégias de transição para criptografia pós-quântica e adaptação de infraestruturas críticas, como mostram publicações do *National Institute of Standards and Technology* (NIST), do *National Cyber Security Centre* (NCSC) e da *Agence Nationale de la Sécurité des Systèmes d'Information* (ANSSI) [Moody et al. 2024, NCS 2025, ANS 2023, Barker et al. 2025]. Para o Estado brasileiro, esse movimento reforça a necessidade de combinar segurança criptográfica, autonomia tecnológica e controle institucional sobre plataformas de comunicação.

Este artigo tem dois objetivos principais: i) discutir a soberania digital estatal, com ênfase na atuação de nações estrangeiras sobre dados, infraestruturas e serviços críticos, e ii) apresentar o ecossistema soberano de comunicações brasileiro, concebido para elevar o controle nacional sobre identidades digitais, bibliotecas criptográficas, sistemas e plataformas de hardware. O trabalho situa o ecossistema proposto como resposta técnica e institucional a um problema estratégico mais amplo.

O restante do artigo está organizado da seguinte forma. A Seção 2 discute soberania digital estatal, seus níveis, exemplos internacionais e o contexto brasileiro. A Seção 3 apresenta o ecossistema soberano de comunicações e seus principais componentes. A Seção 4 aborda seu funcionamento. Por fim, a Seção 5 apresenta as conclusões.

## 2. Soberania Digital

Soberania digital pode ser entendida como a capacidade de um Estado tomar decisões autônomas sobre sua infraestrutura digital e sua implementação tecnológica em território nacional [Pohle and Thiel 2020]. Mais do que posse física de ativos, envolve escolhas sobre arquiteturas, dependências externas, tratamento de dados e supervisão institucional, sob a ótica do interesse público. Trata-se de atributo graduado, observável em níveis como software, infraestrutura de processamento e armazenamento, comunicações, hardware, cadeia de suprimentos, governança regulatória e controle sobre dados estratégicos.

Sob essa perspectiva, soberania digital depende de autonomia tecnológica e controle sobre infraestrutura e dados, sem implicar autarquia. Requer capacidade de compreender, auditar, adaptar, substituir e sustentar tecnologias sensíveis, por código aberto com domínio local ou soluções proprietárias sob controle nacional. Também envolvem-se local de processamento, jurisdição do provedor, custódia de chaves criptográficas e risco de acesso extraterritorial a dados. Na Europa, a Regulação Geral de Proteção de Dados — *General Data Protection Regulation* (GDPR) reforçou o controle sobre dados pessoais [União Europeia 2016], enquanto o debate sobre nuvem evidenciou riscos associados ao *Clarifying Lawful Overseas Use of Data Act* (CLOUD Act) e impulsionou arranjos com maior controle público sobre serviços críticos [Congressional Research Service 2018, Commission Nationale de l'Informatique et des Libertés 2024].

Experiências internacionais ilustram essa agenda: na França, o Tchap, operado pela *Direction Interministérielle du Numérique* (DINUM) em infraestrutura estatal, integra uma estratégia de soberania em áreas sensíveis [Tchap / DINUM 2026]; na China, plataformas nacionais, regulação de aplicativos, segurança de dados e controle de transferências internacionais coordenam capacidade tecnológica doméstica, regulação e controle sobre ativos críticos de informação [State Council of the People's Republic of China 2021, State Council of the People's Republic of China 2024].

No Brasil, o tema combina proteção de dados, defesa e infraestrutura. A Lei Geral de Proteção de Dados Pessoais (LGPD) tutela dados pessoais como matéria de interesse nacional [Brasil 2018]; a Lei nº 12.598/2012 reconhece capacidades produtivas e tecnológicas nacionais em setores estratégicos e insere as Empresas Estratégicas de Defesa como instrumentos de preservação de competências sensíveis ao Estado [Brasil 2012]; e iniciativas como a Nuvem de Governo, gerida por órgãos ou empresas públicas como Serpro e Dataprev, expressam a busca por infraestrutura sob controle nacional [Serviço Federal de Processamento de Dados 2026]. Assim, no contexto brasileiro, soberania digital es-

tatal combina governança regulatória, domínio de infraestruturas críticas, fortalecimento de empresas e cadeias tecnológicas estratégicas e operação de serviços essenciais sob controle jurisdicional e técnico próprio, enquadramento no qual se insere o ecossistema soberano de comunicações.

## 3. Ecossistema Soberano de Comunicações

O ecossistema soberano de comunicações, proposto pelo Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações (CEPESC), articula uma Infraestrutura de Chaves Públicas (ICP) soberana, bibliotecas criptográficas próprias, componentes de software de desenvolvimento nacional e plataformas de hardware concebidas no país, com o objetivo de prover identidade digital, proteção de dados e canais seguros de comunicação sob controle nacional. Em vez de tratar esses elementos de forma isolada, o ecossistema os organiza como uma arquitetura integrada, na qual a confiança se estabelece na ICP soberana, as primitivas criptográficas são encapsuladas em bibliotecas especializadas e os serviços finais são disponibilizados por sistemas e dispositivos voltados a diferentes cenários de uso.

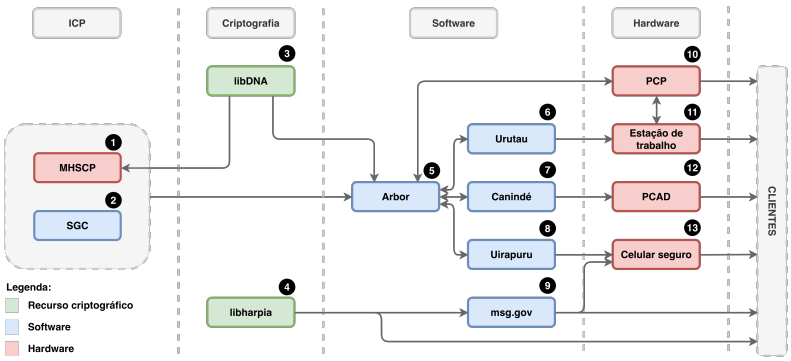


**Figura 1. Visão geral do ecossistema soberano de comunicações e de sua infraestrutura criptográfica.**

A Figura 1 sintetiza essa arquitetura em quatro domínios complementares: ICP, criptografia, software e hardware. Na Subseção 3.1, são detalhados os componentes da ICP soberana, representados pelos itens ❶ e ❷; na Subseção 3.2, são apresentadas as bibliotecas criptográficas correspondentes aos itens ❸ e ❹; na Subseção 3.3, são descritas as soluções de software associadas aos itens ❺ a ❾; e na Subseção 3.4, são discutidas as plataformas de hardware indicadas pelos itens ❿ a ⓭ da Figura 1.

### 3.1. Infraestrutura de Chaves Públicas soberana

Na arquitetura sintetizada pela Figura 1, a ICP soberana[1] é composta pelo Módulo de Hardware Seguro Criptográfico Proprietário (MHSCP) ❶ e pelo Sistema Gerenciador de Certificados Digitais (SGC) ❷. Em conjunto, esses componentes sustentam a raiz de confiança do ecossistema, viabilizando a custódia de material criptográfico sensível e o gerenciamento operacional do ciclo de vida dos certificados.

**MHSCP ❶.** É um Módulo de Segurança de Hardware — *Hardware Security Module* (HSM) adaptado para suportar, além da criptografia de mercado, mecanismos de

[1] A ICP-Brasil já é uma ICP soberana e pode ser perfeitamente adaptada para se aplicar ao contexto deste trabalho.

criptografia de Estado. É nesse equipamento que se concentra a raiz de confiança do ecossistema; por isso, sua implantação deve observar requisitos rigorosos para geração, armazenamento e uso da chave da Autoridade Certificadora (AC) raiz e das demais ACs subordinadas.

**SGC** ❷. É responsável por administrar as chaves criptográficas custodiadas no MHSCP e por operacionalizar os fluxos associados à certificação digital. Além disso, disponibiliza uma Interface de Programação de Aplicações — *Application Programming Interface* (API) por meio da qual o Arbor (ver Seção 3.3) envia requisições e recebe certificados emitidos pelas ACs.

### 3.2. Bibliotecas criptográficas

No domínio criptográfico representado na Figura 1, destacam-se a libDNA ❸ e a libharpia [Pacheco et al. 2022] ❹. Essas bibliotecas concentram a implementação das primitivas criptográficas e expõem interfaces que permitem sua incorporação segura por sistemas de mais alto nível.

**libDNA** ❸. É uma biblioteca compatível com PKCS #11 que pode atuar, por si só, como um *soft token*, permitindo o armazenamento seguro de chaves. Em repouso, seus dados permanecem cifrados com proteção derivada do PIN individual do usuário. Por meio da interface PKCS #11, outras aplicações também podem consumir os serviços criptográficos oferecidos pela biblioteca.

**libharpia** ❹. Fornece uma API de mais alto nível, projetada para reduzir a necessidade de parametrizações manuais por parte do usuário. Seu objetivo é favorecer o emprego consistente de mecanismos criptográficos, evitando que decisões sensíveis, como a escolha de algoritmos e modos de operação, sejam delegadas a aplicações sem o devido controle.

### 3.3. Soluções em software

Na camada de software mostrada na Figura 1, encontram-se o Arbor ❺, o Urutau ❻, o Canindé ❼, o Uirapuru ❽ e o msg.gov ❾. Esses componentes fazem a mediação entre a infraestrutura criptográfica e os ambientes de uso, distribuindo capacidades de identidade, proteção de dados e comunicação segura de acordo com o perfil de cada plataforma.

**Arbor** ❺. Ocupa posição central nessa camada. Sua função é orquestrar o acesso às bibliotecas criptográficas e à ICP soberana, oferecendo uma base comum para os demais sistemas. Entre seus principais módulos, destacam-se: i) Cellulam: *wrapper* implementado em Go para a libDNA, com o propósito de simplificar sua integração com outros sistemas; ii) Cítala: camada construída sobre o Cellulam que expõe os recursos criptográficos para aplicações consumidoras e trata aspectos de concorrência; e iii) Suber: módulo responsável pela comunicação entre o Arbor e a ICP soberana.

**Urutau** ❻. É um Sistema Operacional (SO) hardenizado, baseado na distribuição Debian, concebido para reduzir a superfície de ataque e oferecer um ambiente operacional mais controlado. Ao incorporar as funcionalidades criptográficas providas pelo Arbor, o sistema viabiliza, entre outras capacidades, conexões por Rede Privada Virtual — *Virtual Private Network* (VPN) para clientes com suporte tanto à criptografia de Estado quanto à criptografia de mercado.

**Canindé** ❼. Deriva do Urutau e preserva seus mecanismos de endurecimento, mas é direcionado a equipamentos que operam, principalmente, como servidores VPNs. Por essa razão, contempla adaptações voltadas a cenários de maior demanda de processamento e tráfego de rede.

**Uirapuru** ❽. Também é um SO hardenizado baseado em código aberto, mas voltado ao ecossistema Android. Além da redução da superfície de ataque, sua proposta inclui diminuir a dependência de serviços providos por grandes plataformas digitais, ampliando o controle sobre os dados e a privacidade do usuário.

**msg.gov** ❾. É um aplicativo de mensageria segura que emprega os recursos criptográficos disponibilizados pela libharpia e se apoia no ecossistema Matrix [Martins et al. 2026], cuja arquitetura federada permite a interoperabilidade entre *homeservers* administrados de forma independente. O sistema utiliza os protocolos msgX e msgGX, derivados de Olm e Megolm[2] [Lagrota et al. 2025], respectivamente, com adaptações destinadas a introduzir Criptografia Pós-Quântica — *Post-Quantum Cryptography* (PQC) tanto na negociação quanto na derivação de chaves. O desenho do protocolo prevê uma dupla camada criptográfica: uma baseada em primitivas de mercado e outra em primitivas de Estado.

### 3.4. Soluções em hardware

No domínio de hardware da Figura 1, situam-se a Plataforma Criptográfica Portátil (PCP) ❿, a estação de trabalho ⓫, a Plataforma Criptográfica de Alto Desempenho (PCAD) ⓬ e o celular seguro ⓭. Esses elementos materializam, em plataformas específicas, as capacidades criptográficas, de identidade digital e de comunicação segura providas pelo ecossistema.

**PCP** ❿. É uma plataforma portátil que embarca, por meio do Arbor, a libDNA, expondo capacidades criptográficas para cifração e decifração de dados, bem como permitindo o armazenamento perene de chaves, o que faz dela o *token* físico da identidade digital do usuário. Sua autenticidade é fornecida pela ICP soberana, com a qual se integra via Arbor. O dispositivo também dispõe de armazenamento cifrado para transporte seguro de dados e incorpora o protocolo FIDO2 para autenticação.

**Estação de trabalho** ⓫. Utiliza o SO Urutau para oferecer funcionalidades de segurança sem exigir hardware especializado. Quando associada à PCP, viabiliza autenticação via FIDO2, cifração de dados e operação como cliente VPN, usando a PCP como motor criptográfico em hardware.

**PCAD** ⓬. Destina-se principalmente a conexões VPN de alto desempenho, com emprego típico como servidor em arquiteturas em estrela, para criptografar todo o tráfego de uma rede. A plataforma embarca o SO Canindé e obtém suas capacidades criptográficas da libDNA por meio do Arbor, com recursos nativos ou apoio de módulos dedicados baseados em Matriz de Portas Programável em Campo — *Field-Programmable Gate Array* (FPGA) ou Processador Digital de Sinais — *Digital Signal Processor* (DSP). Também é via Arbor que a PCAD encaminha à ICP soberana requisições de certificação digital.

**Celular seguro** ⓭. Serve de base para o SO Uirapuru, ampliando a proteção em relação

[2]Os protocolos Olm e Megolm são baseados no protocolo Signal [Matrix.org 2019, Matrix.org 2022].

a sistemas convencionais. Integrado ao Arbor, pode prover identidade digital. Quando combinado ao msg.gov, protege dados em repouso por meio do sistema operacional e assegura confidencialidade e integridade dos dados em trânsito por meio da aplicação.

## 4. Funcionamento do Ecossistema Soberano de Comunicações

A Figura 2 sintetiza formas típicas de emprego do ecossistema soberano de comunicações. Em todos os cenários, a confiança deriva da ICP soberana, enquanto o Arbor medeia aplicações e bibliotecas criptográficas, viabilizando identidade digital, cifração e canais seguros em diferentes plataformas.

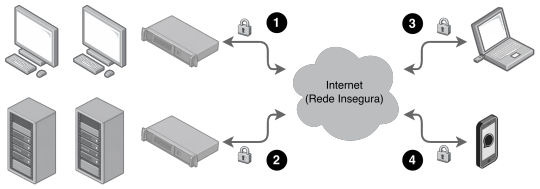


**Figura 2. Diagrama do funcionamento do Ecossistema Soberano de Comunicações.**

Nos cenários ❶ e ❷, a PCAD atua, respectivamente, como cliente VPN em um escritório remoto e como servidor VPN em um Central de Processamento de Dados (CPD). No primeiro caso, usuários de uma rede geograficamente distante acessam, por túneis criptográficos, serviços e aplicações da sede da organização; no segundo, a PCAD concentra múltiplos túneis e controla o ingresso desse tráfego na infraestrutura protegida. No cenário ❸, uma estação de trabalho com o SO Urutau opera com a PCP, combinando endurecimento do sistema, autenticação forte e proteção do material criptográfico no lado do usuário, especialmente em ambientes externos sem garantia de segurança cibernética, como reuniões e missões diplomáticas no exterior.

O cenário ❹ representa o uso do celular seguro com o SO Uirapuru e o msg.gov, estendendo o ecossistema à mobilidade e à comunicação segura. O dispositivo protege dados em repouso, enquanto o aplicativo assegura confidencialidade e integridade das mensagens em trânsito. Em conjunto, os quatro casos mostram que o ecossistema atende ao acesso seguro a redes e serviços e à comunicação protegida entre usuários, preservando controle nacional sobre identidades, chaves e plataformas.

## 5. Conclusão

Este trabalho discutiu a soberania digital como problema tecnológico, regulatório e estratégico, destacando que a dependência de infraestruturas, plataformas e marcos jurisdicionais estrangeiros amplia riscos à proteção de dados, à continuidade operacional e à autonomia decisória do Estado. Nesse contexto, apresentou-se o ecossistema soberano de comunicações brasileiro como arquitetura integrada para prover identidade digital, custódia de chaves, serviços criptográficos e canais seguros sob maior controle nacional. Ao articular uma ICP soberana, bibliotecas criptográficas, sistemas operacionais hardenizados, aplicações e plataformas de hardware especializadas, o ecossistema materializa a soberania digital no acesso seguro a redes e infraestruturas críticas e na comunicação protegida em ambientes móveis. Assim, a proposta fortalece a capacidade estatal ao alinhar segurança, autonomia tecnológica e controle institucional sobre ativos estratégicos de informação.

## Referências

[ANS 2023] (2023). Anssi views on the post-quantum cryptography transition. Technical report, French Cybersecurity Agency (ANSSI). pages 1

[NCS 2025] (2025). Timelines for migration to post-quantum cryptography. Technical report, National Cyber Security Centre (NCSC). pages 1

[Barker et al. 2025] Barker, E., Chen, L., Moody, D., Regenscheid, A., Souppaya, M., Newhouse, B., Housley, R., and Turner, S. (2025). Considerations for achieving crypto agility: Strategies and practices. NIST Cybersecurity White Paper (CSWP) CSWP 39 (2nd Public Draft), National Institute of Standards and Technology (NIST), Gaithersburg, MD. pages 1

[Brasil 2012] Brasil (2012). Lei no 12.598, de 21 de março de 2012. Acesso em: 9 maio 2026. pages 2

[Brasil 2018] Brasil (2018). Lei no 13.709, de 14 de agosto de 2018: Lei geral de proteção de dados pessoais (lgpd). Acesso em: 9 maio 2026. pages 2

[Commission Nationale de l'Informatique et des Libertés 2024] Commission Nationale de l'Informatique et des Libertés (2024). Cloud: the risks of a european certification allowing foreign authorities access to sensitive data. Acesso em: 9 maio 2026. pages 1, 2

[Congressional Research Service 2018] Congressional Research Service (2018). Law enforcement access to overseas data under the cloud act. Acesso em: 9 maio 2026. pages 1, 2

[Grover 1996] Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219. pages 1

[Lagrota et al. 2025] Lagrota, V., Maia, G., Rego, P., Pacheco, R., Macêdo, J. A., and Dantas, M. (2025). msgx: a national digital sovereignty matter. In *Simpósio Brasileiro de Cibersegurança (SBSeg)*, pages 344–345. SBC. pages 5

[Martins et al. 2026] Martins, J. A. P., Rego, P. A. L., de Macêdo, J. A. F., et al. (2026). Matrix protocol: a comprehensive systematic mapping study. *Journal of Cloud Computing*, 15(1):20. pages 5

[Matrix.org 2019] Matrix.org (2019). Olm: A cryptographic ratchet. `https://gitlab.matrix.org/matrix-org/olm/-/blob/master/docs/olm.md`. libolm repository. pages 5

[Matrix.org 2022] Matrix.org (2022). Megolm group ratchet. `https://gitlab.matrix.org/matrix-org/olm/-/blob/master/docs/megolm.md`. libolm repository. pages 5

[Moody et al. 2024] Moody, D., Perlner, R., Regenscheid, A., Robinson, A., and Cooper, D. (2024). Transition to post-quantum cryptography standards. Technical report, National Institute of Standards and Technology (NIST). pages 1

[Pacheco et al. 2022] Pacheco, R., Braga, D., Passos, I., Araújo, T., Lagrota, V., and Coutinho, M. (2022). libharpia: a new cryptographic library for brazilian elections. In

*Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg)*, pages 250–263. SBC. pages 4

[Pohle and Thiel 2020] Pohle, J. and Thiel, T. (2020). Digital sovereignty. *Pohle, J. & Thiel*. pages 2

[Serviço Federal de Processamento de Dados 2026] Serviço Federal de Processamento de Dados (2026). Nuvem de governo. Acesso em: 24 maio 2026. pages 2

[Shor 1997] Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509. pages 1

[State Council of the People's Republic of China 2021] State Council of the People's Republic of China (2021). China regulates apps' collection of personal information. Acesso em: 9 maio 2026. pages 2

[State Council of the People's Republic of China 2024] State Council of the People's Republic of China (2024). China issues regulations on network data security management. Acesso em: 9 maio 2026. pages 2

[Tchap / DINUM 2026] Tchap / DINUM (2026). À propos de tchap. Acesso em: 9 maio 2026. pages 2

[União Europeia 2016] União Europeia (2016). Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 (general data protection regulation). Acesso em: 9 maio 2026. pages 1, 2