CONTRIBUTION TO PUBLIC CONSULTATION:

BRAZIL'S NATIONAL DATA CENTRE POLICY – "CONNECTIVITY AND INFRASTRUCTURE"

1. What principles, values and strategic pillars should guide a national data centre policy to ensure its alignment with national interests and sector challenges? (e.g. Data sovereignty, economic development, innovation)

A National Data Centre Policy must be guided by 3 central principles:

- **Competition, transparency and equity**: the sector is highly concentrated in large providers (Microsoft, Google, AWS). Their hyperscale offerings make it difficult for new competitors to enter. There are also indications of practices such as speculative capacity reservation, generating artificial scarcity. It is essential to ensure transparency in capacity allocation and prohibit artificial reservations.
- **Sustainability**: data centres consume large volumes of energy and water, aggravating their scarcity in some areas. The expansion focused on AI requires robust environmental rules, efficiency targets and public access to information about licenses.
- **Public interest and human rights:** projects must generate local benefits, such as jobs, investments and environmental compensation. They must include prior consultation, environmental compensation measures and restrictions in vulnerable areas, respecting the commitment to sustainable development.

2. What long-term objectives should be pursued to consolidate Brazil as a reference in digital infrastructure?

Brazil's consolidation as a reference in digital infrastructure must be thought beyond the simple attraction of foreign investments in data centre construction. Models based on tax incentives and cheap energy may generate short-term gains but carry the risk of compromising internal expertise and sector governance. The country must prioritise the creation of a transparent, sustainable and human rights-oriented market, strengthening national and regional capacities and attracting a diversity of actors.

It is important to emphasise that dependence on strategic inputs – such as semiconductors and electrical grid capacity – exposes Brazil to geopolitical pressures. The policy must, therefore, advance towards infrastructure self-determination, fostering complete technological ecosystems, reducing vulnerabilities and strengthening national autonomy.

3. What are the main challenges to be faced in the development of the data centre sector?

3.1. What specific guidelines to overcome them effectively?

The data centre sector faces challenges involving competition, sustainability, transparency and socioeconomic impacts. The global market is highly concentrated; this creates entry barriers, lock-in effects and exclusionary practices that limit competition and hinder diversification. In socio-environmental terms, data centres consume a lot of energy and water, especially in hot climates

and regions with water stress, and generate significant emissions and electronic waste, which occurs without transparency or mitigation measures. Additionally, governance and social participation mechanisms are limited or non-existent. As revealed by LAPIN research, environmental impact reports are fragmented and barely accessible, ESG targets often do not reflect real changes, and there is little (or no) consultation with communities. Large-scale projects can aggravate inequalities, increase territorial vulnerability and generate few jobs due to automation of operations.

It is necessary to strengthen the role of competition authorities, eliminating technical, contractual or commercial barriers that hinder migration between providers and ensuring interoperability and freedom of choice for customers.

Detailed, auditable and accessible reports (in different languages) on energy, water consumption and emissions are fundamental, including direct and indirect impacts, disaggregated by region and operation. The focus should be on actual reduction of resource consumption and emissions, with offsets used in a complementary and transparent manner. Data centres must publish water balances, disclose impacts of the mineral extraction chain and waste, and prioritise the reduction or elimination of residual heat.

Permanent channels for social participation must be created, involving local communities, civil society and academia. High-impact projects must include prior consultation, socioeconomic return plans, environmental compensation and restrictions in vulnerable areas.

4. How should this policy articulate with other public policies and/or national development strategies? (e.g. National Artificial Intelligence Strategy, Cybersecurity Policy and Digital Government Strategy).

The policy must be cross-cutting and integrate: National AI Strategy (open data, interoperability and edge computing), Cybersecurity Policy (RPKI/MANRS, incident response), Digital Government Strategy (critical services close to the user), National IoT Plan and spectrum policies (Wi-Fi/6 GHz). Connect to existing initiatives – Digital/Smart Cities, Connected North/Northeast, State Infoways – and to the capillarity of IX.br, expanding regional PTTs and peering incentives to reduce latency, costs and dependence on external routes, strengthening resilience. Prioritise decentralisation with assessment of environmental impacts (energy efficiency, thermal reuse, renewables) and promote neutral and open infrastructure (backbone, backhaul and last mile), including small ISPs and community networks. Finally, IPv6 targets, national CDN/edge and multisectoral governance ensure scale, data sovereignty and continuity.

5. What research and development areas should be prioritised to drive technological innovation in Brazilian data centres?

The current framework for data centre development in Brazil runs the risk of directing substantial resources to solutions that do not address the central problems of market concentration and lack of democratic governance. It is necessary to expand the vision of cloud computing beyond physical infrastructure, considering the entire digital stack and placing fundamental rights and democratic values at the centre. The objective should not be just to build more data centres, but to ensure that

Brazilian digital infrastructure strengthens national sovereignty, protects fundamental rights and preserves the open internet as a space for free expression and information sharing.

7. What are the main challenges and opportunities in the regulatory field for the sustainable and competitive development of data centres in Brazil?

7.1. Does the current legal and regulatory framework offer adequate legal certainty for sector investments and operations?

7.2. Are there norms or legal requirements that hinder or discourage new investments in the sector?

7.3. Are there already existing provisions that have proven effective in promoting the sector and could be strengthened?

It is important to highlight that data centre development cannot be understood separately from cloud service offerings. In the global market, it is observed that hyperscalers, owners of large data centres, also dominate the Software as a Service and Platform as a Service sectors. Without an integrated regulatory strategy, there is a risk that, by seeking to ensure national sovereignty only in the field of physical infrastructure, Brazil ends up deepening dependencies in software layers, equally essential for resilience in service delivery and public policies, especially when linked to the cloud.

Therefore, the regulatory field must evolve to incorporate measures such as:

- **Mandatory risk assessment of dependency on data centres and cloud:** Public institutions and critical infrastructure operators must map their technological dependencies, identifying single points of failure. They must adopt diversification requirements that prevent excessive concentration in one supplier and conduct regular continuity tests to ensure operation during interruptions.
- **Development of governance standards for data centres and cloud**: Create binding oversight structures on market concentration, minimum redundancy standards and interoperability between providers. Include accountability mechanisms for cases of inadequate diversification, in addition to reports on critical dependencies located in foreign infrastructures.

9. How to improve synergy between federal policy and state and municipal initiatives?

Improving synergy between levels of government involves coordination and integration mechanisms that leverage already consolidated experiences. It is essential to ensure that municipal plans dialogue with federal guidelines on connectivity, open data and innovation in public services. Similarly, encouraging neutral infoways, operated in a way that guarantees non-discriminatory access for local providers, strengthens digital inclusion and regional competitiveness.

Another central pillar is strengthening IX.br and the expansion of Traffic Exchange Points (PTTs) at state and municipal levels, which reduces costs, improves critical application performance and

expands infrastructure resilience. Federal policy can support with technical and regulatory incentives, while state and municipal governments collaborate by offering physical infrastructure, energy and institutional partnerships.

10. What mechanisms can ensure transparency, social participation and continuous evaluation of the policy, in order to guarantee its effectiveness and legitimacy over time?

For Brazil to have a coherent and rights-protective National Data Centre Policy, it is essential to ensure transparency, social participation and continuous evaluation. The policy must be developed and revised with consultation mechanisms and public hearings with experts from different areas and diversity of race, gender and region. External audits and multidisciplinary Governance Committees – with representatives from civil society, academia, public and private sectors, and affected people – can monitor its implementation, avoiding episodes such as the installation of TikTok's data centre in Ceará, which occurred without public participation and generated local criticism.

In terms of transparency, there must be a specific portal with information about active data centres in the country, including financial resources, location, responsible parties, social and environmental impacts and mitigation measures adopted. The periodic publication of environmental impact reports and on fundamental rights, as well as complete documentation of processes, is crucial. The policy also needs to incorporate principles of climate justice and protection of traditional and vulnerable communities, preventing digital colonialism practices.

Furthermore, for the policy to be coherent, it is fundamental that Brazil ratify the Escazú Agreement, the first environmental treaty in Latin America and the Caribbean, which seeks to promote rights of access to information, participation and justice on environmental issues, which was signed by Brazil in 2018.

13. Should the policy encourage geographic concentration or dispersion of data centres?

This question requires a nuanced answer, as different types of data centres have distinct technical requirements that guide their location. Edge computing, aimed at content distribution networks and low-latency applications, demands dispersion close to urban centres and end users. Hyperscalers, due to high energy and water consumption and the pursuit of economies of scale, tend to concentrate in locations with favourable infrastructure conditions. More important, however, is avoiding market concentration: a physically dispersed network loses strategic value if controlled by few actors. Thus, the national policy must adopt a hybrid strategy, combining adequate geographic distribution and ownership diversification, to ensure a competitive and resilient digital ecosystem.

14. Should zones of interest be established for data centre installation?

14.1. If so, what criteria should guide the definition of these zones, considering the performance and availability of telecommunications networks?

14.2 What about other conditions, such as energy, climate, security and regional development?

Yes, defining zones of interest can guide investments rationally, ensuring better use of already existing resources and promoting territorial balance. These zones must be conceived in a decentralised manner, avoiding concentration only in large urban centres and reducing vulnerabilities associated with natural disasters or local failures.

The main criteria should include quality and resilience of connectivity, presence of high-capacity backbones, integration with traffic exchange points (IX.br) and availability of multiple fibre optic routes, ensuring redundancy and lower latency. The neutral network policy must ensure that this infrastructure is shared by different operators, expanding competitiveness and reducing interconnection costs.

In addition to connectivity, energy factors (proximity to renewable sources and supply reliability), climate (conditions that favour thermal efficiency), logistics (access roads, water availability and safe routes), as well as social and environmental aspects must be considered. The zones should prioritise areas where data centre installation can generate positive impact on regional development, with creation of qualified jobs, partnerships with universities and valorisation of sustainable practices, avoiding aggravating existing environmental liabilities in sectors such as hydroelectric and wind power.

15. What specific strategies and incentives can be adopted to stimulate data centre installation in less developed regions?

15.1. How can the policy articulate with the economic vocations, geographic characteristics and specific needs of each region?

It is fundamental to seek simpler, decentralised and lower-cost implementation models, suited to local reality. Modular, scalable and lower energy consumption data centres can be encouraged, also favouring alternatives such as neutral networks, open interconnection infrastructures (IX.br), free management software and tools like LibreQoS, which reduce operating costs and avoid excessive concentration in large private providers. Tax and tariff incentives, in addition to public credit lines, can encourage regional providers, cooperatives and community networks to adhere to the model, expanding operator diversity and reducing digital inequalities.

The policy must dialogue with local economic vocations, taking advantage of opportunities in sectors such as agriculture, renewable energy, logistics or digital health. Regions with abundance of clean energy can host more sustainable data centres, while logistics areas can house edge data centres close to the end user. It is equally essential to invest in technical training and regional workforce capacity building, creating courses focused on data centre operation, maintenance and

security. Thus, in addition to ensuring connectivity, local socioeconomic development is promoted, with generation of qualified jobs and reduction of dependence on external infrastructures.

16. How could the existing synergy between fibre optic connectivity in the country's electrical grids and greater decentralisation be enhanced, with the possible location of data centres close to such infrastructures (hydroelectric plants, wind farms, substations, access roads, etc.)?

The use of fibre present in electrical transmission lines can reduce costs and allow greater decentralisation of digital infrastructure. Locating data centres near hydroelectric plants, wind farms, substations and infrastructure corridors offers advantages in energy efficiency and redundancy. However, it is necessary to recognise that many of these areas already concentrate relevant socio-environmental impacts, such as deforestation associated with hydroelectric plants in the Amazon or land conflicts in wind and solar energy regions in the Northeast. The policy must, therefore, combine decentralisation incentives with environmental and social safeguards, encouraging modular data centre models, more efficient in water and energy consumption, and aligned with sustainability policies. Furthermore, the adoption of neutral networks ensures that the connectivity infrastructure associated with these projects is shared fairly, avoiding excessive concentration.

17. In situations of deficit in critical support infrastructure, such as electrical grids, telecommunications and water resources, how to support its development?

Planning must consider that the expansion of energy and telecommunications networks cannot reproduce environmental liabilities already visible in large infrastructure works. In regions with deficits, neutral network and backbone and backhaul sharing policies can reduce the need for new redundant works, while public investments and partnerships can prioritise renewable energies and low environmental impact solutions. In the last mile, small operators and community networks must be supported to ensure capillarity without depending only on large players. Data centres must be conceived in dialogue with local environmental and social characteristics, to avoid overload on water resources, intensive consumption of non-renewable energy or additional pressures on affected communities. Thus, a balance is created between digital resilience, social justice and environmental sustainability.

18. Is it possible to adopt technical standards of quality, security, energy efficiency and environmental sustainability for the different elements that compose data centres, such as physical structure, equipment, software and processes?

It is possible to adopt comprehensive technical standards. The Sustainable Digital Infrastructure Alliance (SDIA), for example, developed a roadmap until 2030 with 21 activities, which include standards for the use of renewable energy, efficient cooling, circular design and hardware standardisation. The World Bank also published a guide that establishes green procurement criteria and sustainable construction standards. These frameworks systematically address the different components of the sector – infrastructure, equipment, software and operations – demonstrating that the adoption of rigorous technical standards is both essential and viable to promote sustainability.

19. How does the quality and resilience of connections affect or encourage data centre deployment?

The decision to install data centres depends directly on the quality and resilience of available connectivity. Regions with unstable networks, little route redundancy or dependence on a single backbone tend to be overlooked, since service continuity is a critical factor. Therefore, it is necessary to ensure rationality in infrastructure planning, prioritising multiple routes, integration with national backbones, interconnection points and presence of high-capacity optical networks. The adoption of neutral network policies is essential so that critical connectivity is shared fairly, allowing the entry of different operators and avoiding excessive concentration in few private actors. In addition to reducing costs and increasing predictability for investors, this approach also favours data centre decentralisation, by creating more balanced market conditions in regions that are currently less attractive.

21. How to strengthen the physical and logistical security of data centres, ensuring data protection and continuity of critical services?

The physical and logistical security of data centres must be part of an integrated territorial strategy. In addition to infrastructure, software dependencies must be considered. Brazil's digital self-determination depends as much on expanding capacity as on reducing vulnerabilities in these layers, which can be as critical as the physicality of the network.

The global outage of July/2024 illustrates this risk: a failure in Microsoft/Crowdstrike cybersecurity software, integrated with Windows, paralysed 8.5 million systems and affected essential services worldwide. The episode shows how cloud software layers can create single points of failure.

The social impact on communities that host these infrastructures must be considered – regarding jobs, training and local partnerships. Planning secure routes, integration with renewable energy, redundancies and rapid response protocols strengthens not only physical protection, but also national resilience.

22. How can the policy promote data centre infrastructure resilience in the face of natural disasters and other contingencies?

Data centre resilience requires decentralisation and redundancy as structuring principles. Concentrating large volumes of processing in few regions increases vulnerability to natural phenomena such as floods, fires or energy failures. The policy must encourage the creation of a network of regional and modular data centres, strategically distributed and interconnected by high-capacity networks, with access guaranteed via neutral network models to avoid monopolies. Thus, dependence on specific hubs is reduced and continuity is ensured in contingency scenarios.

Redundancies must be encouraged at different layers: in energy supply (with renewable sources combined with local backup); in connectivity (with multiple backbones and alternative routes); and in data storage/distribution (with replication in different regions). Thus, greater rapid recovery capacity is guaranteed, with availability of critical services even in the face of crises.