White Paper Data centers

ANATEL

National Telecommunications Agency

SAUS Quadra 6, Blocos C, E, F e H
CEP 70.070-940 - Brasília/DF
Phone: (61) 2312-2000 – www.gov.br/anatel

NATIONAL TELECOMMUNICATIONS AGENCY
Telecommunications Infrastructure Committee

White Paper *Data centers*

Coordinator

Alexandre Reis Siqueira Freire

Brasília – DF

2025

Research team

Coordination
Alexandre Reis Siqueira Freire

Authors

Office of the Director
Alexandre Freire
Alexandre Reis Siqueira Freire
Ailfran Moraes Martins

Superintendence of Competition
Danilo Caixeta Carvalho
Paulo de Avelar Henrique Nicolau

Superintendence of Control of Obligations
Humberto Pontes Silva

Superintendence of Inspection
Gilberto Studart Gurgel Neto
José Umberto Sverzut

Superintendence of Internal Information Management
Breno Cesar Santana Caldas da Silva
Adriano César Dias

Superintendence of Licensing and Resources
Leonardo Marques Campos

Superintendence of Planning and Regulation
Nilo Pasquali
Carolina Henn Bernardi Lellis

Executive Superintendence
Sami Benakouche

Cataloging in publication – Biblioteca da Anatel

W582 White paper data centers [electronic resource] / coordinator: Alexandre Reis Siqueira Freire – Brasília : Anatel, 2025.

1 online resource [43 p.] : il.

Access mode: World Wide Web.
Digital publication (e-book) in PDF format.

Various authors.

1. Data center. 2. Infrastructure. 3. Telecommunication sector. 4. Security. 5. Transparency. 6. Taxation. 7. Government regulation. I. Agência Nacional de Telecomunicações (Brasil). Comitê de Infraestrutura de Telecomunicações. II. Freire, Alexandre Reis Siqueira (coord.). III. Title.

CDD 004.678

Cataloging record prepared by Carolina Pereira Marinho – CRB1/2275

How to cite this book:

FREIRE, Alexandre Reis Siqueira (coord.). **White paper data centers**. Brasília: Anatel, 2025. e-Book. (1 online resource (43 p.)), il.

Summary

1. Presentation 5

2. Introduction 7

3. Overview of Data Centers 9

3.1. Definition and Characteristics of Data Centers 9

3.2. Data center operating models [, , ,] 12

3.3. Contextualization of National and International Scenario 14

3.4. Anatel and Data Centers 16

3.4.1. National data center dashboard: transparency and evidence-based decision-making 20

4. Physical and Cyber Security of Data Centers 21

5. Sustainability and Energy Efficiency of Data Centers 27

5.1. Data centers and ESG (Environmental, social and governance) 28

6. Global Data Center Market 32

7. Data center market in Brazil 34

7.1. Special Taxation Regime for Datacenter Services (Redata) 37

7.2. Subsidy Request - National Data Center Policy 38

8. Challenges and Future Opportunities 39

Challenges to be overcome 39

Future Opportunities 40

9. References 41

1. Presentation

Councilor Alexandre Freire, from April 2023 to July 2024, when reporting on the process of amending the Cybersecurity Regulation Applied to the Telecommunications Sector (R-Ciber), approved by Resolution No. 740, of December 21, 2020, carried out due diligence to the Superintendence of Control and Obligations (SCO) requesting subsidies regarding the use of data centers and cloud computing by telecommunications providers. In response to this request, SCO presented a detailed study on data centers and their relevance in the digital ecosystem and, in its conclusion, among other points, suggested that, considering the progress of other proceedings by Councilor Alexandre Freire related to the topic, the possibility of combining them under the leadership of Anatel's Infrastructure Committee (C-INT) should be evaluated, given that the production of this information is equally important for C-INT.

Thus, within the scope of C-INT, chaired by Counselor Alexandre Freire, the need to delve deeper into the topic was observed, aiming to carry out an accurate diagnosis of the role of data centers in the digital ecosystem, as well as in the design and improvement of sectoral regulation on the subject.

In addition, the Superintendence of Competition (SCP) conducted a specific study on the data center market. The SCO and SCP studies addressed aspects of the evolution and the increasing importance of data centers in the digital age, as well as the structure of the data center industry in Brazil and its impact on the digital ecosystem from an antitrust and competition perspective.

Still with the aim of deepening C-INT's knowledge of data centers, several meetings were held with telecommunications service providers and technology companies to discuss the physical and cyber security of facilities, market growth, location, sustainability, and government support in the context of data centers and cloud computing.

This white paper aims to record and consolidate the information collected by C-INT in both studies and meetings held, in a document that helps to understand the topic

and characterize it as a strategic issue for the entire digital ecosystem, serving as an informative and analytical reference, contributing to the qualified debate on data centers in Brazil.

2. Introduction

The exponential advancement of Information and Communication Technologies (ICT), the growing digitalization of processes, cloud computing, the virtualization of communication network functions (NFV) and the massive use of Artificial Intelligence (AI) have significantly increased the demand for data storage, processing and transmission.

In the coming years, the process of rendering images, videos, and audio will contribute significantly to increased demand for data storage, processing, and transmission in data centers due to the consumption of many machine resources.

Faced with this challenging scenario, data centers take on a strategic role as fundamental elements of technological infrastructure, responsible for supporting increasingly distributed and service-oriented computing architectures. Over the past few years, data centers have undergone a continuous process of evolution, characterized by operational specialization, adoption of emerging technologies, and integration with hybrid and cloud computing models.

The growing demand for high-performance connectivity, AI applications, rendering, energy efficiency, and low latency, driven by the implementation of 5G technology and the expansion of critical digital services, has redefined the parameters for the design, deployment, and operation of data centers. Therefore, data centers are consolidating themselves as essential components of the contemporary digital economy, playing a central role in the implementation of innovative, scalable, and resilient services.

This White Paper aims to provide a detailed analysis of the main aspects related to the regulation and development of the data center sector in Brazil. By addressing important issues such as physical and cyber security, sustainability, energy efficiency, the global and national outlook for the data center market, as well as current challenges and future opportunities, this document provides valuable insights for improving regulatory practices in light of the constant transformations of

the global market, with a view to ensuring a more secure, efficient, and sustainable digital ecosystem, notably the data center infrastructure in Brazil.

3. Overview of Data Centers

3.1. Definition and Characteristics of Data Centers

Data centers are conceived as structures or sets of structures whose main purpose is to centrally host information technology and telecommunications network equipment. These facilities specialize in interconnecting and managing this equipment, offering essential data storage, processing and transmission services.

These structures are undergoing a window of transformation, not necessarily growing in size, but evolving in terms of modernization and diversification. Companies are upgrading their existing data centers and expanding to edge locations, changing the traditional definition of a data center. An example of this transformation is the progressive abandonment of local data centers, due to costs, adoption of cloud computing, and the impact of the pandemic.

Currently, a data center can be a place that hosts IT infrastructure, physical and virtual systems, networks, applications, and support infrastructure. The following types are cited as examples of models:

- Colocation data centers: owned by independent providers, where several organizations host their IT infrastructure. This allows companies to rent space, power, cooling, and other services, enabling more efficient IT operations;
- Hyperscale data centers: operated by large providers such as AWS, Microsoft, Google, and Meta; and focused on virtualized services for corporate clients. Demand for these data centers continues to grow, especially in hybrid cloud computing environments;
- Cryptocurrency data centers: used for cryptocurrency mining. With cryptocurrencies being banned in some countries, these data centers are becoming popular, especially in the US, due to their specific power and hardware requirements;
- Core and Edge Data Centers: located in metropolitan areas. They are used for data exchange between networks, clouds, and corporate digital infrastructure; and

- Cloud data centers: allows the rent of both space and infrastructure. Cloud providers maintain large data centers with security and compliance. This infrastructure can be accessed through various services that offer greater flexibility in usage and payment[1].

The evolution of data centers is also driven by software technology, with machine learning (ML) and AI systems improving efficiency and reducing costs. Interconnection between different data center models is a key trend, integrating physical and virtual IT infrastructures.

Data centers are emerging as **vital components of the critical infrastructure of the digital ecosystem**, acting as neural hubs where data is processed, stored, and distributed. They are fundamental to the functioning of this ecosystem, supporting a wide range of digital activities, from simple data storage to complex cloud computing operations[2]. Firstly, they are essential for data processing and storage, meeting the growing demand generated by the massive volume of information, ensuring that it is handled safely and efficiently. In addition, data centers play a key role in supporting cloud computing, which is an increasingly important component of the digital economy.

Observing the rapid development of this sector, on the one hand, organizations are gaining efficiency and scalability thanks to this evolution and, on the other, providers of these services are facing several challenges to adapt to more sustainable parameters. In a report released in the first half of 2024, the International Energy Agency (IEA) highlighted the forecast of unprecedented growth in global demand for electricity, which could more than double by 2026, due to the advancement of data centers, cryptocurrency mining, and artificial intelligence. The Agency estimates that over the next two years, global electricity consumption by data centers will be between 620 and 1,050 terawatt-hours (TWh), depending on the level of technological evolution over that period, with the highest growth figure being equivalent to the energy demand of highly developed countries, such as Germany and Japan.

---

[1] Amazon. **What is a Data Center?**. Available at: <https://aws.amazon.com/pt/what-is/data-center/>.

[2] Cisco. **What Is a Data center?**. Available at: <https://www.cisco.com/c/en/us/solutions/data-center-virtualization/what-is-a-data-center.html>.

Resilience and security are other important attributes of data centers, designed to ensure high availability and robust protection, which are critical aspects for preserving the integrity and continuity of communications and digital services. It should also be noted that the scalability and flexibility offered by data centers, especially when associated with the use of cloud computing, are essential for agile adaptation to emerging demands resulting from the rapid digital transformation of society.

With the growing volume of data required to train complex AI models, data centers provide the storage and processing capacity needed to handle this demand.

It is important to add that the advent of rendering processes has substantially altered the role and performance of data centers geared toward such applications, which consume high workloads, mainly because they are associated with visual applications, which include videos, 3D images, films, games, design and architecture.

These new processes have become so relevant and essential that they have led to adaptations and adjustments in the performance characteristics of data centers, which began to use GPU components – Graphics Processing Units, in addition to the traditional CPUs – Central Processing Units, working together and acting as performance accelerators.

By augmenting CPUs with powerful parallel processing capabilities and advanced workloads, GPUs accelerate results and ensure greater computing power. Thus, data centers become enabled and capable of operating in emerging AI support technologies, which also include analysis, simulation, modeling, and prototyping processes.

Although GPUs consume more space and energy than CPUs, their incorporation into the new data center environment has become a trend, making them essential to meeting the demands of high computational requirements and growing data volumes, leading to their widespread use in local, cloud, or even virtualized environments.

In the telecommunications sector, the implementation of 5G technology requires lower latency and higher speeds, with data centers and cloud computing playing a

key role in achieving these attributes, enabling new business models such as the management of huge numbers of Internet of Things (IoT) devices and augmented reality, which were previously unthinkable.

3.2. Data center operating models [3, 4, 5, 6, 7]

In simplified terms, we can consider two possible operational models for implementing and operating the computing environment of a data center:

- modern: which uses information technology solutions to employ virtualization, automation and the use of software resources for provisioning, better known by the term infrastructure as code (IaC), and
- Traditional: based on dedicated physical servers and manual management.

Each of these models has distinct characteristics, especially with regard to the delivery of memory, processing, and storage resources, as well as operational aspects such as scalability, provisioning time, resource efficiency, overall performance, and management complexity. In the so-called modern model, memory and processing resources (CPU and GPU) are delivered through virtualization software, which enables the dynamic and on-demand allocation of physical resources made available by server equipment, optimizing the use of physical hardware.

The distribution of storage resources, in turn, is carried out through network solutions, such as SAN (Storage Area Network) and NAS (Network Attached Storage) network elements or even through software-defined storage (SDS) technologies. In a more advanced way, resource delivery can be automated by orchestration tools

---

[3] Barroso, L. A., Clidaras, J., & Hölzle, U. (2013). The Datacenter as a Computer: An Introduction to the Design of Warehouse-Scale Machines (2nd ed.). Morgan & Claypool Publishers.

[4] Hwang, K., Dongarra, J., & Fox, G. C. (2012). Distributed and Cloud computing: From Parallel Processing to the Internet of Things. Morgan Kaufmann.

[5] Patterson, D. A., & Hennessy, J. L. (2017). Computer Organization and Design: The Hardware/Software Interface (5th ed.). Morgan Kaufmann.

[6] Al-Fares, M., Loukissas, A., & Vahdat, A. (2008). A Scalable, Commodity Data center Network Architecture. ACM SIGCOMM Computer Communication Review, 38(4), 63–74.

[7] Villamizar, M., Garcés, O., Ochoa, L., Castro, H., Salamanca, L., Verano, M., ... & Casallas, R. (2015). Infrastructure Cost Comparison of Running Web Applications in the Cloud Using AWS Lambda and Monolithic and Microservice Architectures. Journal of Cloud computing: Advances, Systems and Applications, 4(1), 1–14.

and scripts defined in code, using integrated tools that allow the creation of complete environments in a few minutes, thus establishing an automated infrastructure through programming codes.

The advantages of this model include high scalability, agile and dynamic provisioning, and operational efficiency, since resources are used in an optimized and adaptable manner according to needs, enabling versioning, traceability, and reproducibility of environments through the use of IaC resources. However, this model has some disadvantages, such as management and operational complexity, due to the need for advanced technical knowledge and the possibility of unforeseen provisioning, directly impacting the performance of the environment or critical applications.

In the traditional model, which operates with dedicated physical servers, known as bare-metal, memory and processing resources (CPU and GPU) and storage are allocated physically and statically, where each application is installed directly on the server's operating system and scalability depends on the acquisition and installation of new dedicated physical servers. In this model, storage resources are generally deployed locally, through internal disks on each server, or provided by SAN or NAS networks manually configured in a physical and dedicated storage solution. Resource provisioning is performed by people and the processes are entirely manual, involving the configuration of partitions and volumes.

The main advantage of the traditional model is its high overall performance, due to the absence of provisioning layers for virtualization or operating system resources for this purpose, with greater predictability and physical control of resources, making it more suitable for environments with stricter controls, whether for regulatory or information security reasons. Its disadvantages are significant, implying low flexibility, delay in environment provisioning and underutilization of hardware, increasing the risk of human error.

Table 1 – Comparison between data center operating models

Criteria / Model	Modern model	Traditional model
CPU/GPU/RAM Delivery	Virtualized (on demand);	Physical (fixed per server);
Storage Delivery	Automated; SAN/NAS network; Software-defined networking;	Manual; Local; SAN/NAS;
Scalability	High (with the possibility of orchestration); Insertion of new hardware;	Low (requires insertion of new hardware);
Provisioning time	Minutes;	Days or weeks;
Resource efficiency	High (with the possibility of improper allocation, given the automation);	Low (idle resources);
Performance	Medium (with risk of automatic over-allocation);	High;
Management complexity	High;	Medium.

3.3. Contextualization of National and International Scenario

As already mentioned, the exponential advancement of technology and the growing digitalization of processes have significantly increased the demand for data storage and processing, with a tendency towards increasingly intensive use of edge computing and the massive use of AI.

As connections between systems, people, processes, locations, and devices expand and become more complex, the economic value of the network to each organization increases, while its level of security and management become more costly, strategic and complex.

The digital ecosystem is a complex and dynamic environment made up of several interconnected players that work together to create, deliver and capture value from digital products and services. The value chain of this ecosystem, which is not static, represents the sequence of activities that transform ideas and resources into digital solutions for consumers.

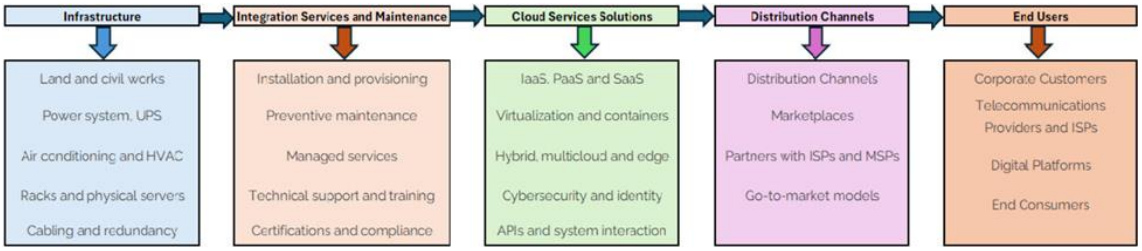
Figure 1 – Digital Ecosystem Value Chain

Source: Study on the Data Center Market in Brazil – Superintendence of Competition (Anatel).

The data center market offers significant economies of scale and scope, resulting in barriers to entry arising from technical and capital-intensive requirements, implying limited capacity for contestation.

Generative AI has significantly impacted the data center value chain, especially due to increased demand for infrastructure, power and cooling requirements, higher bandwidth, and lower latency. This means that all support infrastructure will need to keep up with this demand and flexibility profile, meaning that creating new data centers or updating existing infrastructure will be essential.

Figure 2 Data Center Value Chain



Source: own elaboration

3.4. Anatel and Data Centers

Data centers and cloud computing are emerging as strategic assets in the contemporary digital ecosystem, to the point of being classified as critical infrastructure in many countries. These environments function as neural centers where data is stored, processed, and distributed on a large scale, enabling everything from simple information archiving to complex cloud service operations. Because they support virtually all modern digital activities, they have become fundamental to the functioning of the economy and connected society. Consequently, the resilience and security of these systems are given absolute priority — state-of-the-art data centers must be designed for high availability and robust protection, critical attributes for preserving the integrity and continuity of the communications and digital services they support.

Aware of this importance, Anatel – as the telecommunications regulatory agency – is responsible for ensuring the security and resilience of data centers and cloud services that make up the digital ecosystem. In this sense, aiming to support Anatel's Board of Commissioners with updated information on the topic, Anatel's Infrastructure Committee (C-INT) identified the need to deepen the analysis of the role of data centers in the sector.

Considering these studies, the first concrete action was taken within the scope of the process that amended the Cybersecurity Regulation Applied to the Telecommunications Sector (R-Ciber), approved by Anatel Resolution No. 767, of August 7, 2024, in which Anatel's Board of Commiossioners determined that telecommunications providers include, in their security policies, criteria for contracting data center and cloud computing services – such as the assessment of

the supplier's capacity and practices, risk mapping and degree of dependence. This measure acts as an indirect regulation of these environments, forcing telcos to manage the risks of critical third parties and to select cloud providers diligently. The second action was carried out recently, during the Reassessment of the Regulation for Conformity Assessment and Approval of Telecommunications Products, approved by Anatel Resolution No. 780, of August 1, 2025, where the Agency's Board of Commissioners decided that data centers that integrate telecommunications networks are subject to conformity assessment and approval by Anatel. The specific rules for carrying out this assessment will still be issued by the Agency's technical area.

Furthermore, item 3 of Anatel's 2025-2026 Regulatory Agenda includes the reassessment of the Cybersecurity Regulation applied to the Telecommunications Sector, which has within its scope the evaluation of normative aspects related to data centers and cloud computing, when associated with the telecommunications sector.

In summary, Anatel has been working on both standardization and monitoring of the sector, encouraging the adoption of high standards of security and resilience in these environments that support critical digital infrastructure.

The rapid advance of digitalization brings new regulatory challenges for Anatel regarding data centers and cloud computing. One of these challenges is ensuring interoperability between platforms: the various cloud systems and data center infrastructures must operate in an integrated and standardized manner, avoiding excessive dependence on a single supplier (vendor lock-in) and facilitating data and application portability.

Another crucial concern relates to data sovereignty. It is imperative to ensure that sensitive information and essential services of the country can be stored and processed within national territory, under Brazilian jurisdiction, reducing geopolitical risks and meeting legal data protection requirements. Currently, it is estimated that around 60% of Brazil's digital traffic is handled by data centers abroad (notably in the United States), which means that an interruption in access to these foreign centers could paralyze vital services — it would not be possible to carry out banking transactions via PIX, access SUS medical records, or even operate air transport systems (CONVERGENCIA, 2025).

This reality highlights the urgency of expanding domestic processing and storage capacity, as well as establishing robust contingency plans. The issue of latency is quite relevant: advanced applications enabled by 5G, the Internet of Things, and edge computing demand ultra-low response times, which requires distributed data centers close to users and tightly integrated with telecommunications networks. Finally, the interdependence between clouds and telecommunications networks is undeniable—connectivity failures (e.g., in backbones or submarine cables) can widely disrupt cloud services, creating single points of failure. International regulators are already warning that the massive adoption of outsourced IT providers could introduce significant vulnerabilities, requiring appropriate risk management (BUTLER,2025).

On the international scene, there is a clear trend towards treating data centers and cloud services as critical infrastructure components, accompanied by specific regulatory initiatives. In the United States, although the FCC traditionally focuses on telecommunications networks and does not directly regulate data centers, the federal government recognizes the vital nature of these infrastructures. The National Telecommunications and Information Administration (NTIA), for example, referred to data centers as "the backbone of a secure and resilient technology ecosystem," highlighting their essential role in the digital economy (NTIA, 2024). Additionally, bodies such as the Cybersecurity and Infrastructure Security Agency (CISA) have been publishing guidelines to strengthen the protection of these environments (for example, mitigating vulnerabilities in internet-connected power and HVAC systems), although such measures are still voluntary and not direct regulatory impositions on the private sector (DORNER, 2025).

In the United Kingdom, the government has made progress in institutionalizing the issue: in 2024, data centers were officially classified as Critical National Infrastructure, supporting the expansion of Ofcom's (the British communications agency) jurisdiction to oversee the cybersecurity and resilience of these facilities, under a new legal framework under development (BUTLER,2025). The European Union has explicitly incorporated cloud providers and data centers into its cybersecurity legislation through the NIS2 Directive (EU, 2024), which defines these companies as operators of essential services. The European agency ENISA works to support the implementation of this directive – including the creation of a pan-European registry

of data center and cloud service providers – and to issue technical guidance to raise the level of security and resilience in these sectors (ENISA, 2023). In summary, the main international regulators (such as the FCC, Ofcom, and ENISA) see data centers and cloud computing as critical elements of the digital economy and have been adopting measures to integrate them into national cyber resilience policies. This scenario demonstrates that Anatel's actions and decisions regarding data centers associated with telecommunications networks, aiming to strengthen the resilience and security of critical infrastructure to ensure the availability and continuity of communication services, are in line with international best practices.

However, considering the use of data centers in other contexts, such as banking and government services, it is essential to consider this critical data center and cloud computing infrastructure in a coordinated manner. Firstly, close coordination between the various competent entities is recommended—involving Anatel, national cybersecurity authorities (such as GSI/PR, responsible for cybersecurity policy), the National Data Protection Authority (NDPA), and technological planning and development bodies—in order to align strategies and avoid gaps in action. The development of a National Data Center Plan, already discussed within Anatel, stands out as an important step in this strategy (FERREIRA, 2024). This plan should establish incentives for the installation of data centers in strategic locations throughout the territory, deconcentrating the capacity currently located mostly in the Southeast Region and bringing it closer to the demands of other regions, which would reduce latency, add geographic redundancy, and increase the overall resilience of the system. Furthermore, clear guidelines regarding the storage of sensitive data on Brazilian soil would strengthen digital sovereignty, aligning the country with international best practices in data protection and privacy. Economic obstacles must also be addressed: incentive measures (e.g., tax breaks, easier financing, or reduced charges) can make investing in data centers in Brazil more competitive, helping to reverse the current situation in which local services can cost up to 60% more than in centers abroad — which leads companies to keep a large part of their workloads outside the country (GROSSMANN, 2025).

Finally, it is recommended that data center resilience be integrated into national cybersecurity and essential service continuity plans. This includes ensuring that critical sectors (such as finance, healthcare, telecommunications, and government)

have redundant infrastructure and contingency plans based on national data centers. Such measures must be in line with the National Cybersecurity Strategy (E-Ciber) and other operational continuity regulations, so that data centers are taken into account in incident preparedness and service maintenance under any circumstances. By adopting these initiatives—interagency coordination, promotion of local infrastructure, and incorporation of data centers into security and continuity policies — Brazil will be able to increase the robustness and autonomy of its digital ecosystem, reducing external dependencies and ensuring the continuous provision of critical services to society.

3.4.1. National data center dashboard: transparency and evidence-based decision-making

In this context, Anatel will adopt a more comprehensive, strategic and integrated regulatory stance in monitoring data centers that comprise or perform essential functions in the telecommunications infrastructure. The Agency recognizes that such assets constitute vital elements for the resilience, availability and security of digital services, functioning as true pillars of the national connectivity ecosystem.

With a view to ensuring greater transparency, predictability, and regulatory intelligence, an interactive dashboard will be implemented that will allow for the cataloging, classification, monitoring, and continuous analysis of these data centers. This tool will enable the identification of geographic concentrations, the mapping of risks arising from local vulnerabilities, and the promotion of public policies aimed at promoting territorial diversity and the decentralization of critical infrastructure.

The system will also enable evidence-based decision-making by both the Agency and other sector agents, strengthening the state's ability to anticipate challenges, promote corrective measures, and stimulate innovation. The public availability of information, in an accessible and up-to-date format, reinforces Anatel's commitment to regulatory modernization, the protection of critical infrastructure, and the promotion of a secure, resilient, and sustainable digital environment.

This is, therefore, an initiative that combines technical rigor with strategic vision, aligning with international best practices and helping Brazil consolidate its position as a leading player in the digital economy.

4. Physical and Cyber Security of Data Centers

The construction and operation of data centers are governed by a series of international and national norms and standards. They ensure the quality, safety, efficiency, and sustainability of data centers. The main applicable standards and norms are highlighted below:

- ANSI/BICSI 002-2019 Data Center Design and Implementation Best Practice: This standard provides comprehensive guidance for the design and implementation of data centers. Covering aspects such as physical infrastructure, security, and energy efficiency, it is a vital resource for ensuring up-to-date and efficient practices in data center development.

- ANSI/BICSI 009-2019 Data center Operations and Maintenance Best Practices: Focused on operations and maintenance, this standard addresses best practices for ensuring the continuous and efficient operation of a data center. It includes guidelines on preventive maintenance, fault management, and sustainable operations.

- ANSI/TIA 942B Telecommunications Infrastructure Standard for Data centers: This standard highlights the importance of telecommunications infrastructure in data centers. It specifies requirements for the design and installation of infrastructures that support multiple telecommunications and IT systems, covering aspects such as physical space, layout, cabling, reliability levels (tiers) and environmental considerations. It is a globally adopted standard for data center planning and design.

- ISO/IEC 22237 Information technology – Data centre facilities and infrastructures: The ISO/IEC 22237 series establishes international standards for data center facilities and infrastructure. It covers everything from design and construction to operation and maintenance, focusing on aspects such as energy, environment, and safety.

- ABNT NBR ISO/IEC 22237 Information technology – data center facilities and infrastructure: It is the Brazilian adaptation of the ISO/IEC 22237 series, bringing international standards to the national context, considering local particularities in the construction and operation of data centers in Brazil.

- Uptime Institute Data center Site Infrastructure Tier Standard: A globally recognized standard that classifies data centers into four tiers (Tier I-IV), based on availability, redundancy, and other critical factors.

TIER STANDARDS, created by the Uptime Institute, can be considered today one of the main global standards for data center construction. It establishes the architectural, mechanical, electrical, and communication criteria for building a data center with four security levels: Tier 1, Tier 2, Tier 3, or Tier 4, the latter being the most resilient. This standard has three types of certification:

- Data center project certification (Tier Certification of Design Documents – TCDD).
- Data center infrastructure certification (Tier Certification of Constructed Facility – TCCF).
- Data center operation certification (Tier Certification Operational Sustainability – TCOS).

This allows for the evaluation of various levels of performance, taking into account both the built environment and the approach and performance of the operations team. In summary, while Tier standards establish the design and operating procedures for each Tier classification level, Tier Certification verifies the application of these standards to ensure that the facility is designed, constructed and operated according to the established specifications.

According to the Uptime Institute, the most prevalent certification in data centers in Brazil is TIER III and only two data centers received TIER IV certification, both for the "Tier IV Certification of Design Documents" and for the "Tier IV Certification of Constructed Facility".

The growing demand for data storage and processing, driven by digital transformation and the expansion of emerging technologies such as the Internet of Things (IoT) and AI, creates a technological scenario where data security and protection in data centers play a crucial role.

These technologies deeply affect how data centers operate, and the adoption of preventive and predictive defense measures through automation is highly recommended, aiming, whenever possible, to eliminate threats, perform tests and simulations, and manage risk exposure, all on an ongoing basis.

Physical security in data centers involves protecting the facilities from physical threats such as natural disasters, intrusions, and sabotage. As previously presented, standards such as TIA-942 provide guidelines for building and maintaining secure data centers, addressing aspects such as location, construction, access control, monitoring, and incident response.

Fire protection is another important aspect of physical security in data centers. While TIA-942 includes requirements for detection and suppression systems, standards such as NFPA 75 and 76, published by the National Fire Protection Association, provide greater detail for IT equipment and telecommunications facilities.

The implementation of layered physical security controls is a recommended practice and includes the use of physical barriers, access control systems, video monitoring, and security personnel. The combination of these controls helps minimize risks and ensure the protection of facilities.

NBR ISO 22313 and NBR ISO 22301 are equally important, as they deal with business continuity management, providing guidelines for the implementation of their systems, aiming to ensure that data centers can continue operating even in disaster situations.

This structure allows for staggered risk mitigation, hindering unauthorized access and increasing the physical resilience of the facility. The integration between physical and logical security is essential to mitigate the risk of data compromise through unauthorized access.

The logical security of data centers involves protecting services, systems, networks, and data against unauthorized access, cyberattacks, leaks, and interruptions, and is equally crucial considering the amount of sensitive data stored and processed in these facilities.

Standards such as ISO/IEC 27001:2022 and ISO/IEC 27002:2022 provide guidelines for implementing information security management systems, addressing aspects such as access control, encryption, monitoring, and incident response.

ISO/IEC 27005 provides guidelines for information security risk management, helping organizations identify, assess, and address risks that may compromise the confidentiality, integrity, and availability of information. The standard is a guide for implementing ISO/IEC 27001, focusing on the risk management approach. In this context, as important as applying risk mitigation controls is, initially, having a complete overview of the information assets that make up your infrastructure.

NIST SP 800-53 and CIS Controls v8 are widely used frameworks for cybersecurity. NIST SP 800-53 provides a catalog of security controls for information systems, while CIS Controls offers a set of best practices for protecting systems and data against cyber threats.

The ZTNA (Zero Trust Network Access) architecture is a relatively recent approach to cybersecurity that assumes that no entity, internal or external, is trustworthy by default, emphasizing the need for continuous identity verification and the application of strict security policies for all access to resources provided by a data center computing environment.

Once again, the layered logical protection approach presents itself as an appropriate solution in the search for reducing the level of cyber risk, in which each layer consists of the implementation of a specific solution aimed at reducing the attack surface.

In this sense, the physical and logical protection approaches presented enable action to detect, protect, and contain threats at different points in the infrastructure, increasing resilience and the ability to respond to current risks.

With the transition from data storage and processing processes, which were previously exclusively managed by companies themselves, to cloud computing-based solutions, cybersecurity faces new challenges and complexities. Although the efficiency and scalability benefits offered by cloud computing are readily apparent, adopting this technology introduces an additional layer of complexity to cyber risk management.

Therefore, as we move forward in this transition from data storage and processing processes to cloud computing-based solutions, the importance of cybersecurity in data centers and cloud computing environments cannot be underestimated. In the

case of telecommunications service providers, understanding and proactively addressing the associated cyber risks is crucial to maintaining the traditional trust and integrity of telecommunications systems in society.

Cybersecurity consists of the continuous application of controls designed to mitigate risks against threats that may compromise the confidentiality, integrity, or availability of information assets. In turn, because they house the majority of these assets, data centers become the primary focus of many targeted attacks, which requires a high level of protection and security.

Data centers can contain hundreds to thousands of physical and virtual servers, which are segmented by application type, technology, data classification, and other methods. Creating and managing appropriate security rules to control access to and from resources can be a significant challenge.

It is worth noting that the cybersecurity landscape is dynamic and constantly evolving, and cybercrime, as one form of crime, is increasing considerably, both in terms of investment volume and sophistication. Thus, protecting information technology infrastructure and digital services is one of the major challenges today, both in terms of technology and skills.

In the context of public administration, the National Cybersecurity Strategy (E-Ciber), established by Decree No. 10,222/2020, and the National Information Security Policy (NISP) are fundamental documents that guide the implementation of information security management.

Guided by these instruments, Brazil relies on a normative and operational structure provided by the Presidency of the Republic, through the Institutional Security Office (GSI/PR), which plays a strategic role in coordinating information security in the country. The GSI/PR is responsible for establishing information security guidelines within the Federal Public Administration, especially through the Information Security Department (DSI). The DSI, in turn, publishes technical and operational regulations focused on cybersecurity, such as Normative Instruction GSI/PR No. 1/2020, which establishes criteria for risk management, protection of critical infrastructure and incident response. At the heart of incident response, the Cyber Incident Prevention, Handling and Response Center of Brazilian Government (CTIR Gov.br) acts in the

technical coordination of the containment and mitigation of cyber threats, promoting information exchange and coordination between public agencies within the Federal Cyber Incident Management Network (REGIC).

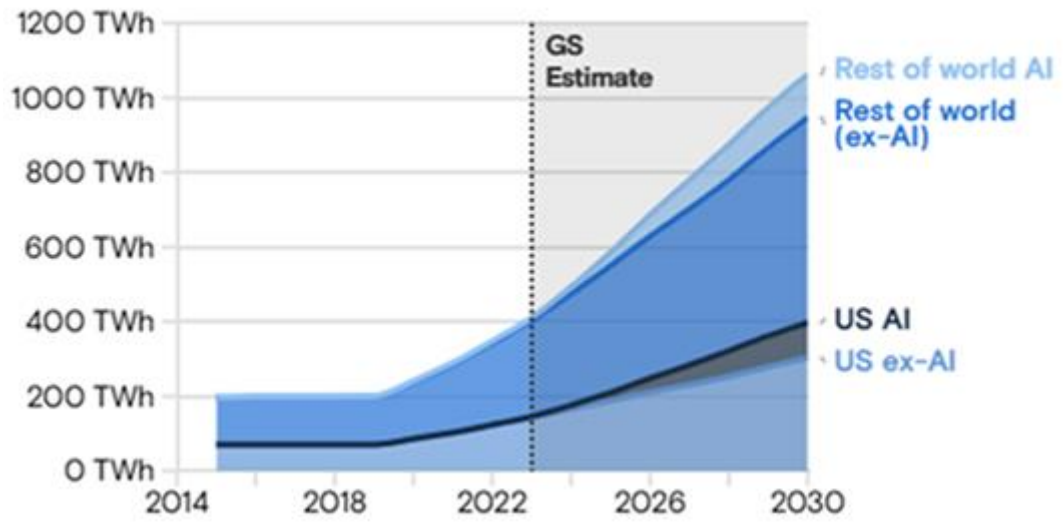
Also noteworthy, specifically for the bodies and entities that are part of the Information Technology Resources Management System (SISP), is the Information Security Protection Plan (PPSI), provided for in Normative Instruction SGD/ME No. 1/2020. The Digital Government Secretariat (SGD), currently linked to the Ministry of Management and Innovation in Public Services (MGI), is responsible for coordinating the implementation of the NISP within the scope of the SISP, promoting guidelines, orientations and structuring actions such as the ISPP itself. This plan seeks to establish a systematic approach to information security management in public agencies, encompassing risk analysis, identification of critical assets, definition of controls, and development of treatment plans. In this context, the Integrated Cybersecurity Center of Digital Government (CISC Gov.br) acts as the Federal Government's sectoral Cyber Incident Prevention, Treatment and Response Team (ETIR), being responsible for coordinating actions for the prevention, detection, analysis and response to cyber incidents involving SISP bodies and entities. The coordination between SGD, CISC Gov.br and SISP bodies contributes to strengthening cyber resilience and the State's coordinated response capacity to digital threats.

5. Sustainability and Energy Efficiency of Data Centers

Data centers are major energy consumers. Energy is used to power servers, storage systems, networking equipment, and, significantly, the cooling systems needed to keep the equipment at optimal operating temperatures.

Currently, data centers consume 1 to 2% of the world's energy, and this demand is expected to increase to 3 to 4% by the end of the decade.

Figure 3 – Data Center Energy Demand



Source: https://www.goldmansachs.com/insights/articles/AI-poised-to-drive-160-increase-in-power-demand

This increase in energy consumption, and consequently in carbon dioxide (CO_2) emissions due to data centers, will represent a social cost of US$ 125 to 140 billion (in present value). Understanding this social cost, although complex to quantify, is essential to promoting sustainability and mitigating the negative impacts of the growing demand for digital infrastructure. The transition to renewable energy sources and the implementation of energy efficiency practices are crucial to reducing the social cost of carbon associated with data center operations.

According to the Uptime Institute, energy costs can represent up to 44% of a data center's total operating costs, making energy efficiency a crucial factor for the business's economic viability.

Thus, the massive use of energy and its environmental impacts have led the industry to invest in innovative and efficient facilities, including new refrigeration technologies and the use of sustainable and renewable energy sources, such as the incorporation of low-consumption technologies and advanced refrigeration systems, in addition to the migration to renewable energy sources.

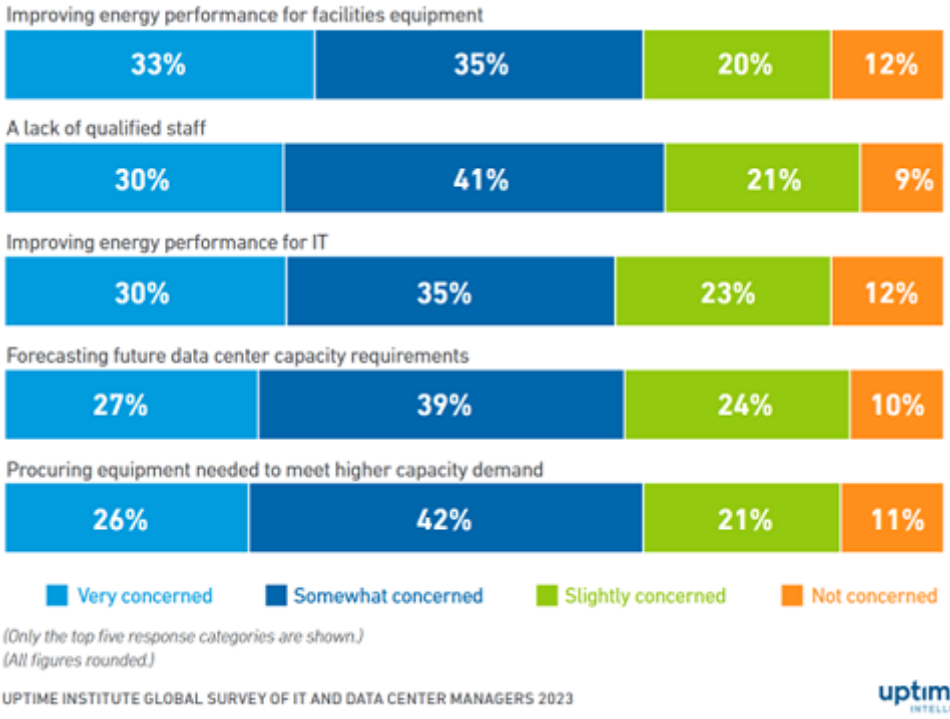
5.1. Data centers and ESG (Environmental, social and governance)

The Uptime Institute Global Data center Survey[8] published in 2023 highlights a growing industry that is crucial in scale and importance, but faces an increasingly wide range of challenges. Data center operators now face stricter regulations and the need to reduce energy consumption. At the same time, challenges related to human resources and the supply chain persist. Although new technologies are emerging as promising solutions, they are expensive and still lack standardization and scalability. The study also reveals that the global Power Usage Efficiency (PUE) index in data centers has remained stable over the past four years, indicating that further improvements in this indicator will require significant investment.

More than half of data center operators reported outages at their facilities in the last three years, maintaining a trend of steady improvement. Female participation in the data center workforce is only 8%, a figure lower than in sectors such as mining and construction in the US. Corporations identify the privacy and confidentiality of their data as the main obstacle to migrating storage and processing of data considered critical to the public cloud.

[8] UPTIME INSTITUTE – Global Data center Survey 2023 – available at link

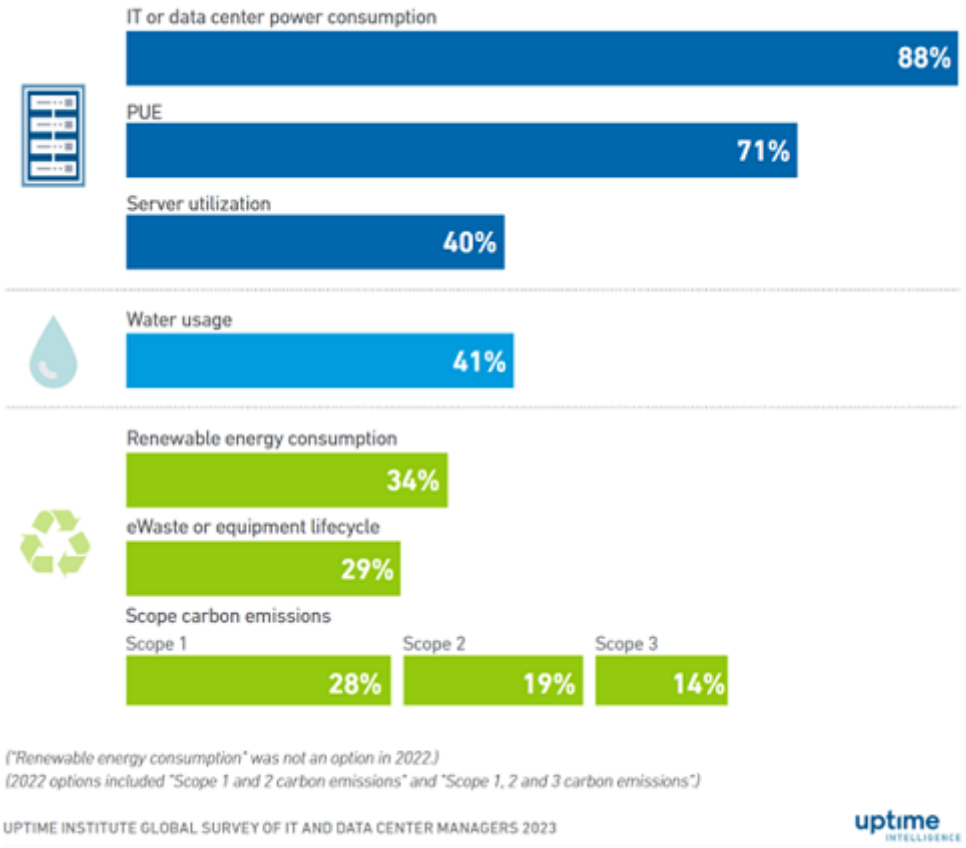
Figure 4 – Top concerns for the next 12 months [Research] [Source: Uptime Intelligence]



Furthermore, the same study presented a survey of 629 digital infrastructure managers. The main concerns for the next 12 months are hiring staff and energy efficiency. This figure reflects the current challenges facing the sector in securing a qualified workforce and improving sustainability and energy efficiency in data centers. These factors are fundamental to the functioning and continued growth of global digital infrastructure.

The survey of managers indicates that many data center operators will likely struggle to meet increasing sustainability reporting demands from both customers and the general public.

Figure 5 – Top priorities in corporate sustainability reports [Source: Uptime Intelligence]



Another survey reveals that energy consumption in IT and data centers is considered a top priority in corporate sustainability reports. According to this survey of 716 participants, this prioritization reflects the growing importance of efficient energy management and sustainability in the sector. IT and data center managers compile and report on a variety of metrics for corporate sustainability purposes, with a significant focus on energy consumption, demonstrating an ongoing effort to optimize resource use and reduce environmental impact.

Finally, according to Uptime Intelligence, nowadays, the focus on sustainability reports is more on the efficiency of infrastructure operations, such as in terms of energy and water, than on reducing carbon emissions. This can be interpreted as a choice by data center operators to monitor the amount of work, such as a server's CPU cycles, which can be derived from a resource, such as a unit of energy, rather than assessing the carbon emissions impact related to the generation of that energy resource. This approach is likely adopted due to the fact that improvements in energy and water consumption often result in financial savings. The prospect of

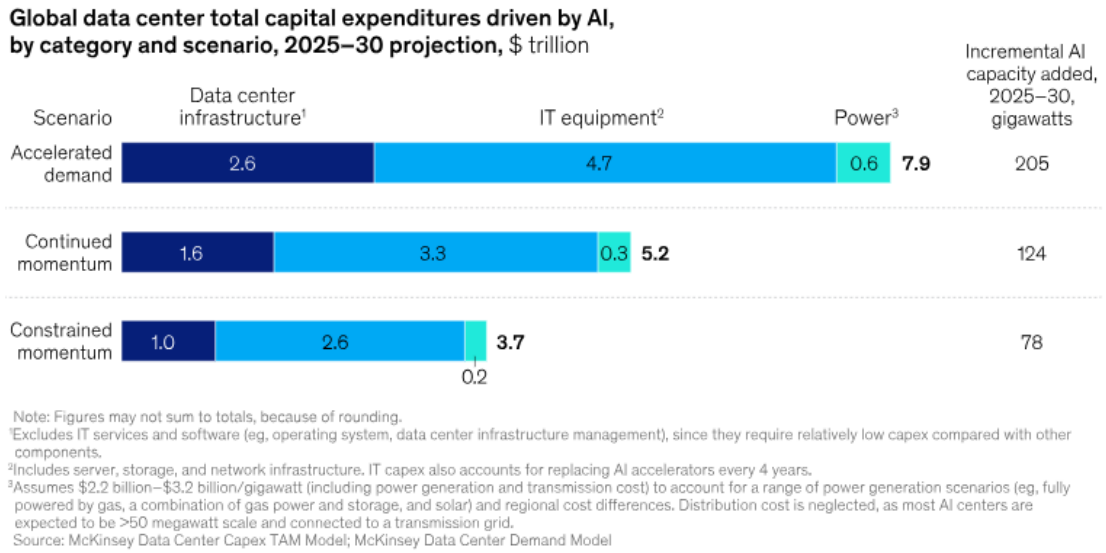
reducing carbon emissions is more complex, as it is not limited to managing consumption and, for this reason, is not directly related to financial savings.

6. Global Data Center Market

In order to meet the growing demand for services hosted in data centers, investments of between US$ 3.7 and 7.9 trillion are estimated for data centers between 2025 and 2030.

The global data center market size is expected to grow from USD 242.72 billion in 2024 to USD 584.86 billion in 2032, exhibiting a Compound Annual Growth Rate (CAGR[9]) of 11.6%.

Figure 6 – Global data center investment estimates

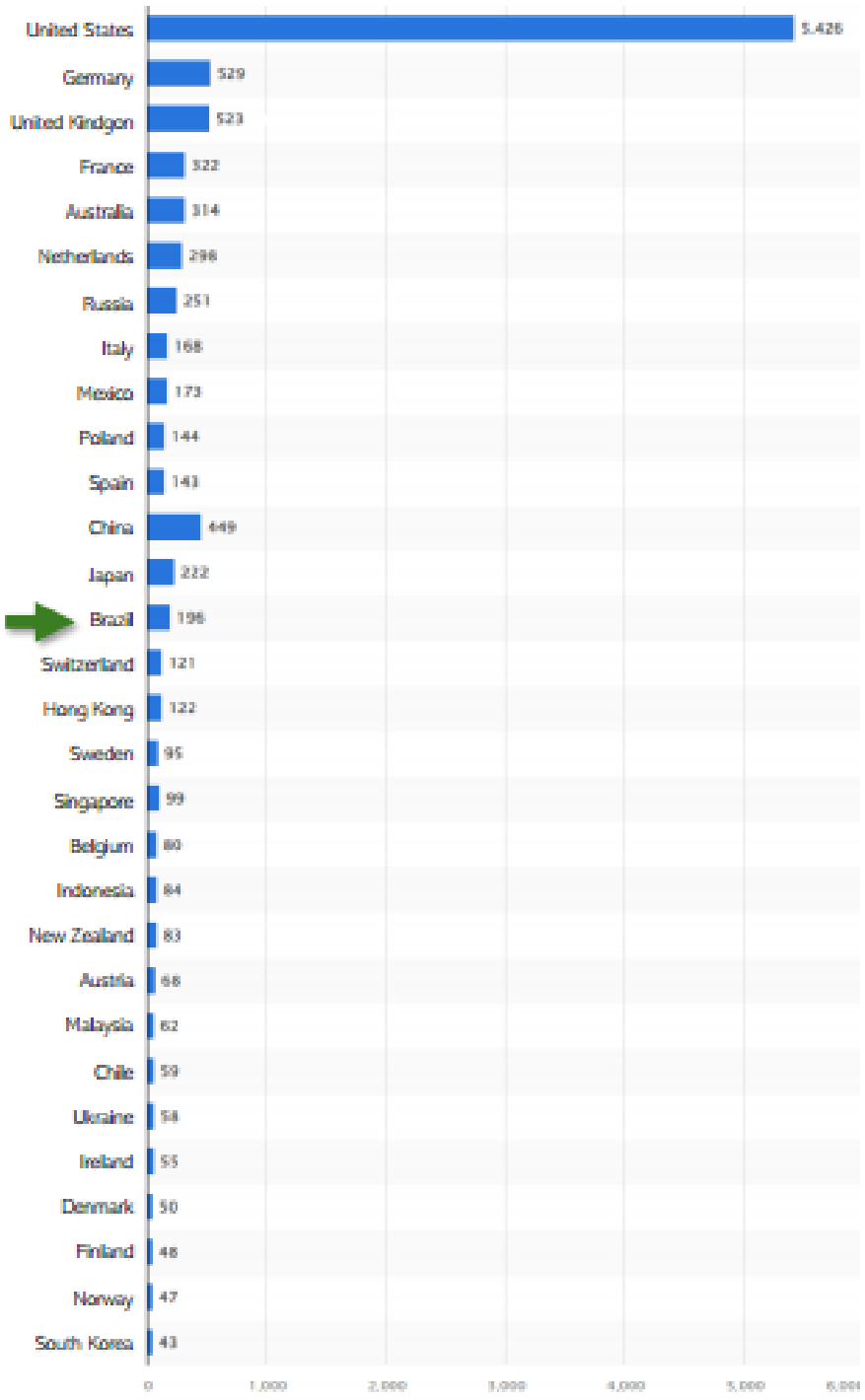


Source: https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/the-cost-of-compute-a-7-trillion-dollar-race-to-scale-data-centers

Currently, the largest numbers of data centers are located in the United States, Germany, the United Kingdom, and China. Brazil, with 196 data centers, occupies a relatively prominent position in the global distribution of this infrastructure.

[9] CAGR calculates the average annual growth rate of an investment, taking into account reinvestment of earnings

Figure 7 – Global Distribution of data centers



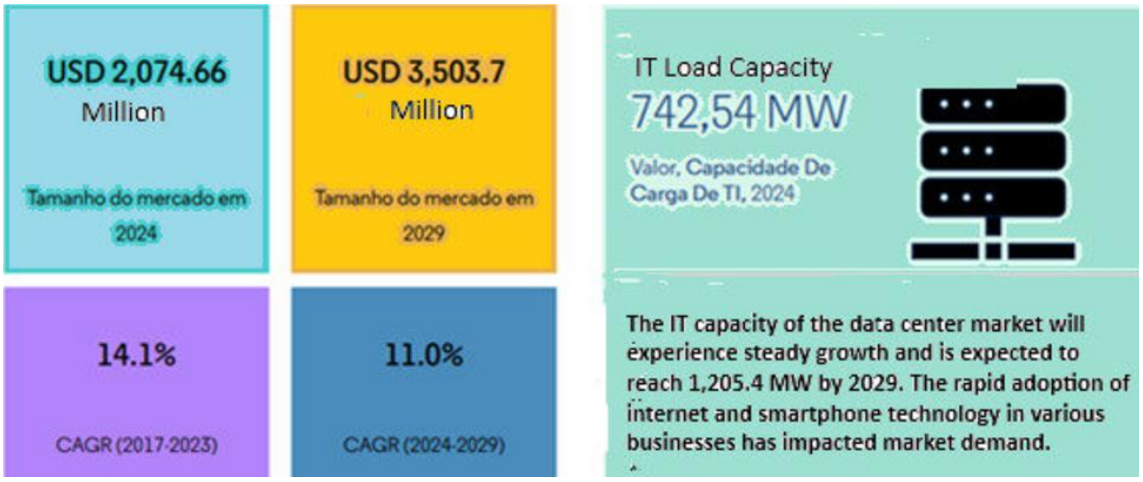
Source: https://www.statista.com/statistics/1228433/data-centers-worldwide-by-country/

7. Data center market in Brazil

The data center market in Brazil is experiencing a period of accelerated expansion, driven by digital transformation, migration to the cloud, and increased data traffic. Investments are estimated to reach US$3.5 billion per year in the country[10], representing an increase in IT power of 1,500 MW over the next 5-10 years.[11].

The data center market in Brazil is expected to reach 1,210 MW by 2029, with a CAGR of 10.17% per year. Additionally, colocation revenues are projected to reach US$3.504 billion by 2029, with a CAGR of 11.0%.

Figure 8 – Estimates for the Brazilian data center market



Source: https://www.mordorintelligence.com/industry-reports/brazil-data-center-market

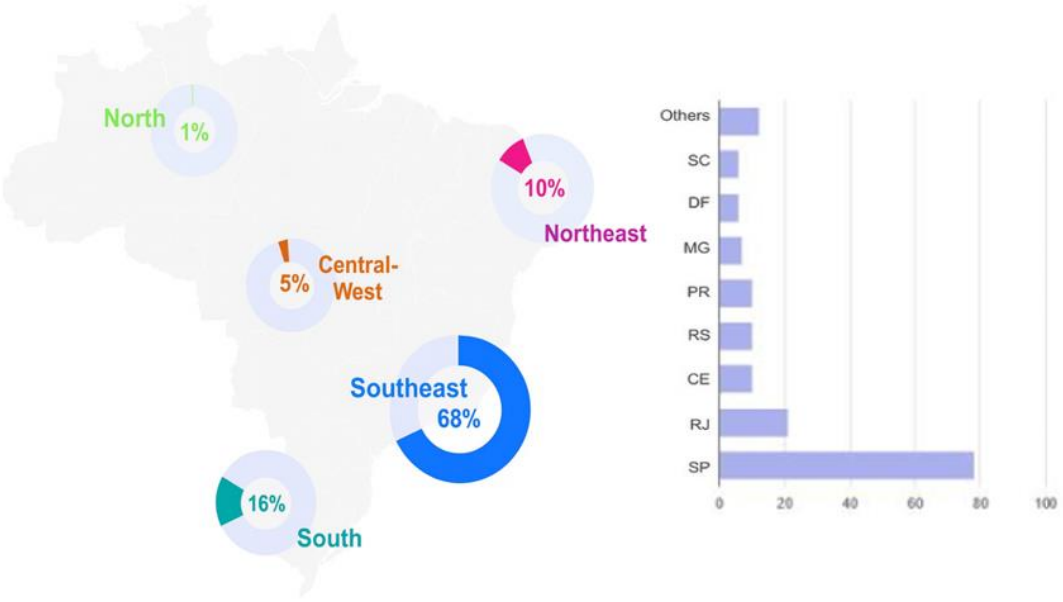
In Brazil, there is a concentration of data centers in the states of São Paulo and Rio de Janeiro due to their robust infrastructure and proximity to the country's major companies and financial institutions. Aiming to reduce latency, there is a trend towards expanding data center infrastructure to regions peripheral to major centers, as well as to regions lacking such infrastructure.

[10] https://agoradistribuidora.com.br/data-centers-a-infraestrutura-fisica-por-tras-da-nuvem-no-brasil/

[11] datacenterdynamics.com

Figure 9 – Distribution of data centers – Brazil

The states of São Paulo and Rio de Janeiro account for most of the country's data centers.
Approximate number of data centers by Brazilian state.

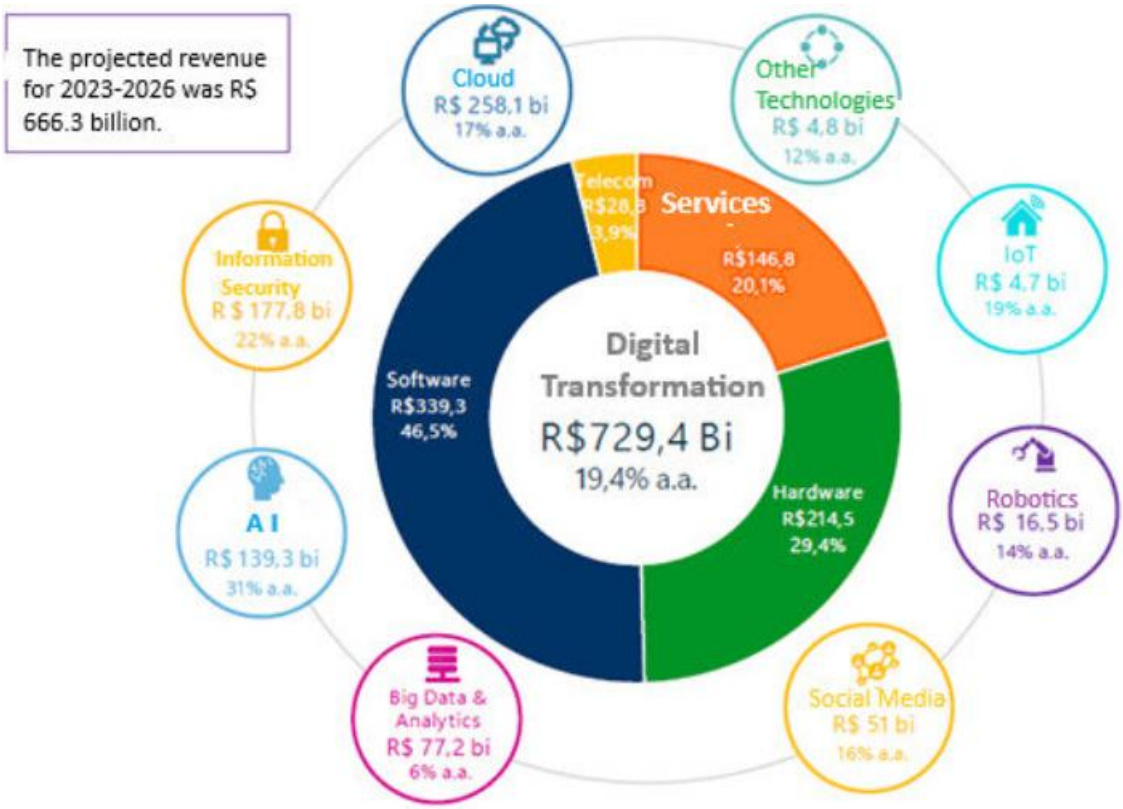


Source: Brazil data Centers e Moody's Local Brasil

The digital ecosystem, where data centers are inserted, represents about 6.5% of the national GDP[12]. Its impact is due to direct investment, the generation of qualified jobs, and, fundamentally, because it is the infrastructure that supports the country's growing digital economy, and it tends to increase with the ongoing digitalization and the advancement of technologies such as AI.

[12] https://www.gov.br/fazenda/pt-br/central-de-conteudo/publicacoes/relatorios/sre/relatorio-economico_plataformas_publicacao_rev.pdf

Figure 10 – Investment outlook – 2024-2027



Source: https://brasscom.org.br/inteligencia/relatorio-setorial/

The costs of installing and operating a data center are high and require significant capital investments which, combined with the different scales of the players involved, in addition to the economic and digital inequality between different regions, can act as a natural barrier to entry into this market.

To finance investments in technological infrastructure, including the construction of new facilities and capacity expansions, data center developers resort to borrowing or private investors, such as private equity and venture capital funds. In Brazil, most data center developers have private equity participation.

This financial dependence exposes data center companies to risks related to macroeconomic conditions, such as interest rates and volatility in financial markets.

In addition to high capital costs, economies of scale can represent significant barriers to entry and expansion of the number of players in this market by providing owners of large data centers with global reach with gains in operating costs. For example,

the cost per kilowatt (kW) of computing capacity tends to decrease as the size of the data center increases.

Furthermore, economies of scope can also be observed, where the combined offer of services, such as connectivity, cloud computing, payment platforms, digital security, software, etc., provided by integrated companies that own data centers, implies cost optimization and customer attraction (trend towards "one place for everything"), resulting in a scenario that is unattractive to the entry of new players.

7.1. Special Taxation Regime for Datacenter Services (Redata)

Provisional Measure (MP) No. 1,318, of September 17, 2025, instituted the Special Taxation Regime for Datacenter Services (Redata), aiming to stimulate the installation and expansion of data centers in Brazil in order to strengthen digital infrastructure and attract investments. The regulation is seen as a necessary tool to compete with international incentive policies and meet the growing demand for connectivity and cloud services.

Strategically, the MP seeks to consolidate Brazil as a hub for the digital economy and ensure digital sovereignty, given that around 60% of Brazilian digital traffic depends on processing and storage carried out abroad. This dependence leads to trade deficits and risks to national sovereignty.

With the incentives provided by Redata, it is estimated that up to R$2 trillion in investments will be mobilized in the data center sector over ten years, considering tax benefits that could reach R$701 billion. Such investments could quadruple the country's processing capacity, from 800 megawatts to up to 3 gigawatts.

The economic impact is based on the granting of exemption from federal taxes (PIS/Pasep, Cofins, IPI and Import Tax) on the acquisition of ICT equipment, which reduces the effective rate from 52% to approximately 18%.

On the other hand, the regime establishes strategic and environmental obligations that become a competitive advantage for Brazil. Beneficiary companies must use clean or renewable energy, meet water efficiency criteria, and invest 2% of the value of the products purchased in research, development, and innovation (R&D) in the

country. Besides, at least 10% of processing capacity must be allocated to the domestic market.

7.2. Subsidy Request - National Data Center Policy

In a strategic initiative, the Federal Government, through the Ministry of Communications, opened a Subsidy Call in August 2025 to hear from society and experts on the infrastructure and connectivity axis of the National Data Center Policy. This public consultation represents a fundamental step towards the development of integrated policies aligned with the sector's demand, and also involves ministries such as the Ministry of Development, Industry, Commerce and Services (MDIC) and the Ministry of Finance.

This initiative is strategic for boosting the economy, attracting investment, and strengthening innovation in the country, and it aims to create an environment conducive to technological development, generating qualified jobs, economic returns, and a legacy that positions Brazil as a global benchmark in the data center sector.

The consultation covers different types of infrastructure, from corporate data centers to hyperscaler cloud computing, which process large volumes of data, as well as edge data centers, which are essential for bringing services closer to users and enabling low-latency technologies, such as self-driving cars, telemedicine, and the Internet of Things. The debate includes topics such as connectivity, sustainability, security, governance, quality standards, strategic location, professional training, and integration with existing public policies, including the National Artificial Intelligence Strategy, the National Cybersecurity Policy, and the Digital Government Strategy.

In this context, Anatel plays a fundamental role in implementing actions that complement and enhance the objectives of the National Data Center Policy. The Agency has been promoting the mapping, cataloging, and monitoring of data centers that integrate or support telecommunications networks, recognizing them as critical infrastructure for the resilience, security, and continuity of digital services. Furthermore, Anatel has been working on classifying and monitoring these environments, considering aspects such as physical and cybersecurity, energy efficiency, sustainability, and adherence to international best practices.

8. Challenges and Future Opportunities

As already mentioned, advances in artificial intelligence and high-performance computing will significantly contribute to the expansion of the data center market by driving investment in infrastructure and the search for global solutions, which, in turn, will encourage technological innovation.

Brazil is consolidating itself as a promising market for data centers, with expectations of reaching up to 1,210 MW by 2029. This growth provides important future opportunities; however, it is necessary to consider the significant challenges that will need to be faced for this consolidation.

Challenges to be overcome

- **High tax burden**: one of the biggest obstacles to the growth of the data center market in Brazil is the high tax burden and other internal factors that make operations in the country more expensive. It is noted, however, that there are already government initiatives addressing this issue, such as the publication of a Provisional Measure on the exemption of data centers, which aims to anticipate the effects of the tax reform with the exemption of federal taxes on investments made by the data center sector.

- **Geographic concentration**: most data centers are concentrated in São Paulo, given the region's high demand for this type of service, and in cities that are anchor points for submarine cables, in order to ensure better connectivity and speed. This geographic concentration raises concerns regarding network security and resilience. The issue is being studied by the Ministry of Communications, which intends to formulate a national policy for submarine cables, with measures to enhance the installation of submarine cables along the Brazilian coast, in addition to encouraging the use of other anchoring points besides those already traditionally used.

- **Entry barriers**: The segment demands technical and capital-intensive requirements, which limits the entry of new players into the market.

- **Qualified workforce**: There is a shortage of qualified professionals in the IT and telecommunications sector, which is an obstacle to the development and expansion of projects.

- **Equipment cost**: Domestic production of data center components is limited, focusing on items more common to industrial facilities, and many critical

components are imported due to the high specialization and low scale of the local market, which represents a higher cost.

- **High energy consumption**: Data centers have very high energy consumption, and energy costs can represent up to 44% of a data center's total operating costs, making energy efficiency crucial. Brazil's energy matrix, while sustainable, can still present supply risks during periods of prolonged drought, given the predominance of energy generated by hydroelectric plants.

Future Opportunities

- **Accelerated segment growth**: The expansion of the data center sector in Brazil, driven by the rise of artificial intelligence, is robust and expected to continue growing, with estimated annual investments of US$3.5 billion in the country.

- **Natural competitive advantages**: Brazil holds around 12% (twelve percent) of the world's fresh water, which is essential for cooling data centers. Besides, the country has great potential for generating clean and renewable energy, such as solar, wind, SHPs (Small Hydroelectric Power Plants) and biomass, being a great attraction for companies that aim to implement ESG practices and seek to reduce their carbon footprint, such as large cloud providers that have goals of 100% renewable energy.

- **Excellent telecommunications infrastructure**: Brazil has an extensive fiber optic network, good backbone infrastructure, and the presence of large telecommunications companies. Another highlight regarding infrastructure is Brazil's connections to international submarine cables, which helps position the country as a strategic location for the installation of data centers.

- **Tax and regulatory incentives**: Rio de Janeiro already offers state tax incentives to attract units, including ICMS reductions, IPTU, ITR and ISS exemptions. There are proposals for a national public policy strategy to attract investment in data centers, including the application of tax incentives for the purchase of IT equipment and energy consumption, benefiting data centers throughout the country during the construction and operation stages.

9. References

1. **MORDOR INTELLIGENCE**. Tamanho e Análise de Participação do Mercado de Data center no Brasil: Tendências e Previsões de Crescimento até 2029. Mordor Intelligence. 2022. Disponível em: https://www.mordorintelligence.com/pt/industry-reports/brazil-data-center-market. Acesso em: 02 jun. 2025.

2. **SOUTO, Poliana**. Notícia: MP para data centers 'está praticamente pronta', diz Alckmin. Megawhat, 2025. Disponível em: https://megawhat.energy/economia-e-politica/mp-para-data-centers-esta-praticamente-pronta-diz-alckmin/. Acesso em: 04 jun. 2025.

3. **MINISTÉRIO DAS COMUNICAÇÕES**. Notícia: Tomada de Subsídios sobre a Política Nacional de Cabos Submarinos. MCom - Secretaria de Telecomunicações, 2025. Disponível em: https://www.gov.br/participamaisbrasil/mcom-tomada-subsidios-cabos-submarinos. Acesso em: 13 maio 2025.

4. **MINISTÉRIO DAS COMUNICAÇÕES**. Notícia: Tomada de Subsídios - Política de Data Centers Eixo CI. MCom - Secretaria de Telecomunicações, 2025. Disponível em: https://www.gov.br/participamaisbrasil/tomada-de-subsidios-sobre-a-politica-nacional-de-data-centers. Acesso em: 13 out. 2025.

5. **MINISTÉRIO DO DESENVOLVIMENTO, INDÚSTRIA, COMÉRCIO E SERVIÇOS**. Estudo: Estratégia para Implementação de Política Pública para Atração de Data centers. MDIC e ABDI, 2023. Disponível em: https://www.gov.br/mdic/pt-br/assuntos/sdic/comercio-e-servicos/comercio/estudo_completo_datacenters_jun2023.pdf/view. Acesso em: 07 abr. 2025.

6. **MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS**. Tomada de subsídios sobre a Política Nacional de Data Centers. Disponível em: https://www.gov.br/participamaisbrasil/tomada-de-subsidios-sobre-a-politica-nacional-de-data-centers/. Acesso em: 13 out. 2025.

7. **MIRAE ASSET AP RESEARCH TEAM**. The Trends that will Shape the Data Centre Market in 2020. Mirae Asset, 2022. Disponível em: https://www.am.miraeasset.com.hk/insight/the-trends-that-will-shape-the-data-centre-market-in-2020/. Acesso em: 17 mar. 2025.

8. **MCKINSEY & COMPANY**. The cost of compute: A $7 trillion race to scale data centers. McKinsey & Company, 2025. Disponível em: https://www.mckinsey.com/industries/technology-media-and-

telecommunications/our-insights/the-cost-of-compute-a-7-trillion-dollar-race-to-scale-data-centers#/. Acesso em: 05 maio 2025.

9. **FORTUNE BUSINESS INSIGHTS**. Tamanho do mercado de data center, análise de participação e indústria: Período de Estudo 2019-2032. Fortune Business Insights, 2023. Disponível em: https://www.fortunebusinessinsights.com/pt/data-center-market-109851. Acesso em: 16 jun. 2025.

10. **AGORA DISTRIBUIDORA**. Data centers: a infraestrutura física por trás da nuvem no Brasil. Agora Distribuidora, 2024. Disponível em: https://agoradistribuidora.com.br/data-centers-a-infraestrutura-fisica-por-tras-da-nuvem-no-brasil/. Acesso em: 19 mar. 2025.

11. **LOMBARDI, Alessandro**, Quais fatores tornam o Brasil um mercado atraente para investimentos em data centers? Elea Digital Data centers. 2023. Disponível em: https://www.datacenterdynamics.com/br/opini%C3%B5es/quais-fatores-tornam-o-brasil-um-mercado-atraente-para-investimentos-em-data-centers/. Acesso em: 04 jul.2025.

12. **STATISTA**. Leading countries by number of data centers as of March 2025: Survey time period 2025. Statista, 2025. Disponível em: https://www.statista.com/statistics/1228433/data-centers-worldwide-by-country/. Acesso em: 26 jun. 2025.

13. **BRASSCOM**, Relatório Setorial 2023 Macrossetor de TIC. Brasscom, 2024. Disponível em: https://brasscom.org.br/quem-somos/sobre-a-brasscom/. Acesso em: 17 fev. 2025.

14. **MINISTÉRIO DA FAZENDA**. Plataformas Digitais no Brasil: Fundamentos Econômicos, Dinâmicas de Mercado e Promoção de Concorrência. Secretaria de Reformas Econômicas, 2024. Disponível em: https://www.gov.br/fazenda/pt-br/central-de-conteudo/publicacoes/relatorios/sre/relatorio-economico_plataformas_publicacao_rev.pdf. Acesso em: 27 mar. 2025.

15. **SOUSA, Roberto**, Eficiência Energética em Data centers no Brasil. Bravo Tecnologia. 2024. Disponível em: https://bravotecnologia.com.br/eficiencia-energetica-em-data-centers-no-brasil/. Acesso em: 04 jul. 2025.

16. **AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES**. Notícia: Conselho Diretor aprova Proposta de Alteração do Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações. 2024. Disponível em https://www.gov.br/anatel/pt-br/assuntos/noticias/conselho-diretor-aprova-proposta-de-alteracao-do-regulamento-de-seguranca-cibernetica-aplicada-ao-setor-de-telecomunicacoes. Acesso em: 13 ago. 2025.

17. **AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES**. Notícia: Anatel aprova novas regras para certificação de produtos. 2025. Disponível em https://www.gov.br/anatel/pt-br/assuntos/noticias/anatel-aprova-novas-regras-para-certificacao-de-produtos. Acesso em: 13 ago. 2025.

18. **AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES**. Notícia: Implantação de data centers no Brasil é objeto de debate na Anatel. 2025. Disponível em https://www.gov.br/anatel/pt-br/assuntos/noticias/implanatacao-de-data-centers-no-brasil-e-objeto-de-debate-na-anatel. Acesso em: 13 ago. 2025.

Siga a Anatel