

DATA CENTERS NO BRASIL:

ANÁLISE DO *WHITE PAPER* DA ANATEL

Este ebook apresenta uma análise sistematizada do *white paper* elaborado no âmbito do Comitê de Infraestrutura de Telecomunicações da Agência Nacional de Telecomunicações (Anatel) sobre data centers no Brasil. O documento, lançado em 13 de outubro, aborda conceitos, tendências tecnológicas, referências regulatórias nacionais e internacionais, padrões de segurança física e cibernética, informações sobre sustentabilidade e dinâmica de mercado, além de propor diretrizes para aprimorar a resiliência, a competitividade e a soberania digital do país.

1. CONTEXTO E RELEVÂNCIA

Data centers e serviços em nuvem compõem a infraestrutura crítica da economia digital que viabiliza desde aplicações essenciais de governo, saúde e sistema financeiro até novos casos de uso que demandam baixa latência e alto poder computacional – como aqueles que envolvem 5G, Internet of Things (IoT), renderização intensiva e inteligência artificial.

A crescente interdependência entre nuvem e redes de telecomunicações tem aumentado a importância de abordagens regulatórias integradas, de gestão de riscos de terceiros e de políticas públicas voltadas à expansão segura, sustentável e descentralizada da capacidade instalada no Brasil.

2. PRINCIPAIS ACHADOS

2.1 Modelos operacionais e evolução tecnológica

O *white paper* distingue dois modelos operacionais possíveis de implantação e operação: o modelo ancorado em virtualização, automação e infraestrutura como código, com ganhos de escalabilidade e eficiência, e o modelo tradicional (*bare metal*), com alocação estática de recursos e maior previsibilidade de desempenho.

O relatório da Anatel compara os dois modelos, como mostra a tabela abaixo:

Tabela 1 - comparativa de critérios operacionais

CRITÉRIO / MODELO	MODELO MODERNO	MODELO TRADICIONAL
Entrega de CPU / GPU / RAM	Virtualizada (sob demanda);	Física (fixa por servidor);
Entrega de Armazenamento	Automatizada; Rede SAN/NAS; Rede definida por software;	Manual; Local; SAN/NAS;
Escalabilidade	Alta (com possibilidade de orquestração); Inserção de hardware novo;	Baixa (exige a inserção de hardware novo);
Tempo de provisionamento	Minutos;	Dias ou semanas;
Eficiência de recursos	Alta (com possibilidade de alocação indevida, face a automatização);	Baixa (recursos ociosos);
Desempenho	Médio (com risco de super alocação automática);	Alto;
Complexidade de gestão	Alta;	Média.

Além dos modelos operacionais, o *white paper* destaca os principais tipos de data center e suas características, usos típicos e implicações de conectividade, energia e governança:

- **Colocation:** é de propriedade de provedores independentes, que alugam espaço, energia, refrigeração e serviços gerenciados. O modelo *retail* atende múltiplos clientes em menor escala; o *wholesale* viabiliza grandes salas ou andares dedicados. Esse tipo de data center se beneficia de economia de escala, diversidade de carriers e acesso a pontos de troca de tráfego (IXs). Os contratos variam por potência (kW/MW), acordo de nível de serviço (SLA) e serviços adicionais (*remotes hands*, *cross-connects*).
- **Hiperescala:** instalações de grande porte, altamente padronizadas e automatizadas, operadas por provedores globais. Suportam nuvem pública, plataformas e serviços massivos. Demandam terrenos extensos, várias subestações, linhas dedicadas e soluções avançadas de refrigeração e eficiência (PUE baixo). A densidade por rack tende a crescer com cargas de IA (GPU-densas).
- **Nuvem:** opera com oferta de recursos como serviço (IaaS/PaaS/SaaS), com elasticidade e faturamento por uso. A nuvem pública roda majoritariamente em data centers hiperescaláveis. A nuvem privada pode residir em instalações proprietárias ou *colocation*. Arquiteturas híbridas/*multicloud* exigem interoperabilidade, portabilidade e gestão de riscos de terceiros críticos.
- **Borda/Edge:** localizados em áreas metropolitanas, próximos do usuário/antena para reduzir latência e backhaul, que suporta 5G, IoT, vídeo e casos de uso sensíveis ao tempo (telemedicina, indústria 4.0). Costumam operar com energia e espaço limitados, exigindo soluções compactas, automação e resiliência local.

Essas tipologias coexistem em arquiteturas híbridas, integrando-se por interconexões físicas e lógicas. A escolha do tipo depende de requisitos de latência, densidade, compliance, custos (Capex/Opex), maturidade de automação e estratégia de soberania e portabilidade, com impactos diretos sobre segurança, continuidade e eficiência energética.

2.2 Referências regulatórias internacionais

O *white paper* aponta que existe uma convergência global para o tratamento de data centers e nuvem como infraestrutura crítica.

Nos Estados Unidos, diretrizes de resiliência e segurança são impulsionadas por órgãos federais, ainda que sem regulação setorial direta, já que a Comissão Federal de Comunicações (Federal Communications Commission – FCC) regulamenta as telecomunicações no país.

No Reino Unido, data centers foram formalmente classificados como infraestrutura nacional crítica, o que amplia a supervisão sobre cibersegurança e resiliência.

Na União Europeia, a Diretiva NIS2 inclui provedores de nuvem e data centers como operadores de serviços essenciais, com apoio técnico da Agência da União Europeia para a Cibersegurança (European Union Agency for Cybersecurity – Enisa). Essas experiências reforçam padrões de segurança, continuidade e governança que servem de referência para o Brasil.

2.3 Atuação regulatória da Anatel

O *white paper* indica que a Anatel vem adotando medidas normativas e de monitoramento com impactos diretos no ecossistema digital:

- O primeiro movimento da Anatel nesse sentido foi a alteração do Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações (R-Ciber), aprovada pela Resolução Anatel 767/24. A alteração estabelece que prestadoras incorporem critérios de contratação de serviços de data centers, avaliação e gestão de riscos de terceiros críticos (data center e nuvem).
- Outra ação relatada no *white paper* se refere à Reavaliação de Avaliação da Conformidade e Homologação de Produtos para Telecomunicações, aprovada pela Resolução Anatel 780/25. A norma abrange data centers integrados às redes de telecomunicações e os torna passíveis de avaliação da conformidade e de homologação pela Anatel.
- O *white paper* também indica que consta da Agenda Regulatória da Anatel a inclusão de data centers e cloud no seu escopo, especificamente no eixo de cibersegurança.
- Outra medida é a implementação de um *dashboard* nacional para catalogação, classificação e monitoramento de data centers críticos, para apoiar a tomada de decisão baseada em evidências e facilitar a descentralização geográfica.

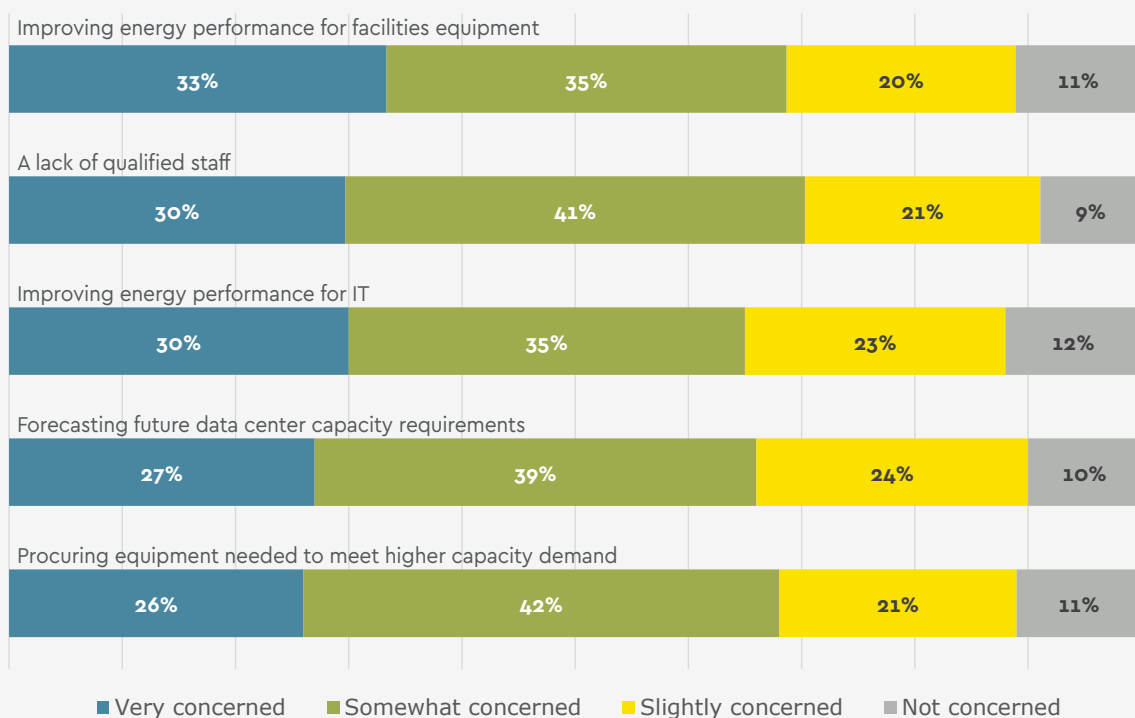
2.4 Segurança física e cibernética

O *white paper* consolida padrões amplamente adotados, incluindo TIA-942, ISO/IEC 22237 (e NBR correlata), BICSI 002/009, NFPA 75/76, ISO/IEC 27001/27002/27005, NIST SP 800-53, CIS Controls v8 e práticas de Zero Trust. Destaca-se a prevalência de Tier III no Brasil, com poucos casos Tier IV. Recomenda-se adotar defesa em camadas, integração entre segurança física e lógica, automação e gestão contínua de riscos, além de aderência a normas de continuidade (NBR ISO 22301/22313).

2.5 Sustentabilidade e eficiência energética

Data centers consomem entre 1% e 2% da energia global, com projeção de 3% a 4% até o fim da década. Os custos com energia podem representar até 44% dos custos totais da operação de um data center, o que torna críticas estratégias de eficiência, resfriamento avançado, otimização hídrica e contratação de fontes renováveis. Há pressão crescente por transparência em métricas ESG, ainda que a mensuração e padronização de emissões de carbono diretas permaneçam desafiadoras.

O *white paper* mostra as principais preocupações para os próximos 12 meses (ou seja, para o ano de 2026):



(Only the top five response categories are shown.)

(All figures rounded.)

UPTIME INSTITUTE GLOBAL SURVEY OF IT AND DATA CENTER MANAGERS 2023

uptime
INSTITUTE

2.6 Mercado global e nacional

Há previsão de investimentos globais na ordem de trilhões de dólares entre 2025 e 2030 e de crescimento do mercado de aproximadamente US\$ 243 bilhões (2024) para US\$ 585 bilhões (2032). Atualmente, os maiores polos incluem Estados Unidos, Alemanha, Reino Unido e China.

No Brasil, estima-se que haverá investimentos em torno de US\$ 3,5 bilhões/ano e expansão de potência de TI de 1,5 GW nos próximos anos, com projeção de 1,21 GW até 2029 e grande crescimento anual em colocation. Persistem como pontos de atenção a elevada concentração geográfica em São Paulo e dos pontos de ancoragem de cabos submarinos, além de barreiras de capital, escala e mão de obra qualificada.

2.7 Políticas públicas e soberania digital

Em 18 de setembro de 2025, foi editada a Medida Provisória 1.318/25, que instituiu o Regime Especial de Tributação para Serviços de Datacenter (Redata). O novo regime visa incentivar a instalação e ampliação de data centers, oferecendo benefícios fiscais, como a suspensão de tributos na aquisição de equipamentos de

tecnologias da informação e comunicação (TIC). A concessão de benefícios fiscais é condicionada a uso de energia limpa, eficiência hídrica, pesquisa e desenvolvimento (P&D) doméstico e reserva de capacidade para o mercado interno.

Espera-se que, nos próximos dez anos, sejam realizados investimentos de até R\$ 2 trilhões em data centers no Brasil, com vantagens tributárias significativas para companhias do setor.

Paralelamente, o governo federal iniciou o processo de tomada de subsídios para a Política Nacional de Data Centers, com foco em conectividade, localização, sustentabilidade, segurança, padrões e capacitação. A tão falada soberania de dados é apontada como prioridade, com base na estimativa de que grande parcela da carga digital brasileira é processada no exterior, o que traz riscos de latência, de continuidade e geopolíticos.

3. DIAGNÓSTICO E LACUNAS

O diagnóstico trazido pela Anatel no *white paper* confirma que os data centers são infraestrutura crítica e que o Brasil vem dando passos regulatórios importantes. Ainda assim, persistem lacunas estruturais e operacionais que, se não tratadas, podem limitar a resiliência, a soberania digital e a competitividade do Brasil.

Apontamos, a seguir, as principais lacunas indicadas no *white paper*.

3.1 Dependência externa e soberania de dados

Estima-se que uma grande parcela das cargas digitais brasileiras ainda é processada no exterior, em especial em nuvens e data centers localizados fora do território nacional. Essa dependência cria riscos operacionais e geopolíticos (interrupções de conectividade internacional, restrições regulatórias extraterritoriais). Há também desafios de interoperabilidade, portabilidade residência de dados sensíveis, planos de contingência e capacidade doméstica para setores essenciais.

3.2 Concentração geográfica e pontos únicos de falha

A infraestrutura nacional permanece concentrada em poucos polos, principalmente na Região Sudeste e em cidades com pontos de ancoragem de cabos submarinos. Essa concentração aumenta a exposição a eventos locais (climáticos, elétricos ou de segurança) e limita a redução de latência para aplicações de 5G, IoT e IA.

A descentralização geográfica (novos polos regionais e arquitetura de borda), aliada à diversificação de rotas de *backbone* e de *landings*, está sendo estudada pelo Ministério das Comunicações. A ideia é formular uma política nacional para cabos submarinos, com medidas que estimulem a instalação desses cabos na costa brasileira. Também se estuda incentivar a utilização de outros pontos de ancoragem, diferentes dos já tradicionalmente utilizados. Com essas medidas, espera-se mitigar riscos sistêmicos.



3.3 Energia: custo, disponibilidade e infraestrutura elétrica

A energia pode representar até 44% dos custos totais da operação de um data center. Isso faz com que custo e previsibilidade de fornecimento assumam um papel crítico. A expansão de cargas GPU-densas para IA eleva a densidade térmica e as exigências de refrigeração (inclusive soluções líquidas ou imersão).

O relatório da Anatel aponta que há desafios de conexão em alta tensão, necessidade de diversos alimentadores, subestações, redundância e acordos de energia renovável com lastro e adicionalidade.

3.4 Barreiras financeiras, escala e cadeia de suprimentos

O setor é intensivo em capital e beneficia grandes players por economias de escala e de escopo (*colocation*, *cloud*, conectividade, segurança gerenciada). A dependência de equipamentos importados faz com que os custos fiquem ainda mais altos e os prazos se alonguem, sujeitando os projetos à volatilidade cambial e a gargalos logísticos.

3.5 Governança, supervisão e transparência baseadas em risco

Tratando-se dos data centers que integram as redes de telecomunicações, a evolução regulatória precisará consolidar uma abordagem proporcional ao risco. Além de incorporar boas práticas de gestão de riscos de terceiros e de continuidade, será necessário fazer a integração com políticas nacionais de cibersegurança.

A iniciativa de *dashboard* nacional é vetor-chave para mapeamento de concentração geográfica, classificação de criticidade, acompanhamento de capacidade/energia e apoio à tomada de decisão pública e privada.

3.6 Latência, edge e integração com redes

Casos de uso sensíveis ao tempo exigem a instalação de data centers próxima ao usuário e forte integração com redes de acesso, transporte e IXPs. Segundo o *white paper*, persistem lacunas na disponibilidade de sites regionais com energia, espaço e conectividade adequados, além de modelos de negócio que viabilizem a operação sustentável dessa presença fora dos grandes centros.

Em síntese, superar essas lacunas passa por três eixos:

- I. ampliar e desconcentrar a capacidade doméstica com energia competitiva e infraestrutura elétrica robusta;
- II. fortalecer a governança de risco, a interoperabilidade e a transparência; e
- III. desenvolver capital humano e cadeias produtivas para sustentar, com qualidade e eficiência, o ciclo de investimentos em curso.

4. ANÁLISE DE RISCOS E IMPLICAÇÕES REGULATÓRIAS

A interdependência entre nuvem e redes pode ampliar riscos sistêmicos decorrentes de falhas de conectividade e de fornecedores críticos.

Segundo estudos apontados no relatório da Anatel, a adoção massiva de terceirização de TI impõe ao regulador e aos operadores medidas robustas de due diligence, gestão de riscos de terceiros e planos de contingência.

A incorporação de data centers a políticas de cibersegurança e continuidade de serviços essenciais é apontada no *white paper* como uma condição para reduzir pontos únicos de falha e vulnerabilidades, especialmente em serviços críticos.

5. RECOMENDAÇÕES

Fortalecer a coordenação entre Anatel, Gabinete de Segurança Institucional da Presidência da República (GSI/PR), Autoridade Nacional de Proteção e Dados (ANPD) e ministérios setoriais é apontado no *white paper* como uma medida importante para alinhar políticas de soberania de dados, interoperabilidade e continuidade de serviços essenciais.

Além disso, o relatório aponta ser necessário estruturar um Plano Nacional de Data Centers com: metas de descentralização geográfica e indução de novos polos regionais e de borda; integração com estratégias nacionais de IA, cibersegurança e governo digital; diretrizes de residência e processamento de dados sensíveis em território nacional; e coordenação com o *dashboard* nacional para mapeamento de criticidade e apoio a decisões públicas e privadas.

6. CONCLUSÃO

O *white paper* elaborado pela Anatel oferece um diagnóstico abrangente e considera que os data centers estão no cerne da transformação digital e da segurança econômica do país. De acordo com a agência, o Brasil dispõe de vantagens estruturais — matriz energética com potencial renovável, disponibilidade hídrica e infraestrutura de telecomunicações — e está construindo um arcabouço regulatório e de políticas públicas que pode atrair investimentos e elevar a autonomia tecnológica. Para materializar esse potencial, a Anatel entende que é essencial consolidar uma agenda integrada de governança, segurança, sustentabilidade e competitividade, com foco na redução de dependências externas, na descentralização geográfica e na resiliência de serviços essenciais, em linha com as melhores práticas internacionais.



A presente Nota Técnica se presta, exclusivamente, a resumir o White Paper – Data Centers de autoria do Comitê de Infraestrutura da Agência Nacional de Telecomunicações. Eventuais opiniões constantes desse documento não representam, necessariamente, as opiniões dos advogados do Escritório.

FALE COM NOSSA ESPECIALISTA



Milene Louise Renée Coscione

Sócia

MCoscione@machadomeyer.com.br

APOIO:

Alessandra Jeronimo Ungria Galvão

Júlia Caffaro Giuzio Dantas

PORTAL INTELIGÊNCIA JURÍDICA

Nossa visão para as questões que impactam seus negócios

Acesse nosso conteúdo: www.machadomeyer.com.br/inteligenciajuridica

MACHADO MEYER ADVOGADOS
SÃO PAULO / RIO DE JANEIRO / BRASÍLIA / BELO HORIZONTE / NEW YORK

MACHADO
MEYER
.COM.BR

