INTERFACE TECNOLÓGICA

TECNOLOGIA EM INFORMÁTICA
Interface Tecnológica · v. 23, n. 1, 2026 · p. 59–68
ISSN on-line 2447-0864 · ISSN impresso 1807-3980
https://doi.org/10.31510/infa.v23i1.2441

DATA CENTERS DE IA: a escassez energética e o risco emergente na segurança da informação

AI data centers: the energy shortage and the emerging information security risk

Luan Gabriel Benfica[1], **Kawan Melo Saraiva Sabino de Sousa**[2], **Rickelmi Henrique Ferreira dos Santos**[3], **João Emmanuel D'Alkmin Neves**[4]

AUTORIA

[1] **Luan Gabriel Benfica**
Fatec Americana – SP – Brasil
luan.benfica@aluno.cps.sp.gov.br
ORCID: https://orcid.org/0009-0006-1748-1818

[2] **Kawan Melo Saraiva Sabino de Sousa**
Fatec Americana – SP – Brasil
kawan.sousa@aluno.cps.sp.gov.br
ORCID: https://orcid.org/0009-0009-0424-2211

[3] **Rickelmi Henrique Ferreira dos Santos**
Fatec Americana – SP – Brasil
rickelmi.santos@aluno.cps.sp.gov.br
ORCID: https://orcid.org/0009-0003-0590-5853

[4] **João Emmanuel D'Alkmin Neves**
Fatec Americana – SP – Brasil
joao.neves@cps.sp.gov.br
ORCID: https://orcid.org/0000-0002-9472-9753

HISTÓRICO

Recebido	26/04/2026
Aceito	04/06/2026
Publicado	30/06/2026

COMO CITAR

BENFICA, L. G. et al. Data centers de IA: a escassez energética e o risco emergente na segurança da informação. **Interface Tecnológica**, Taquaritinga, v. 23, n. 1, p. 59-68, 2026. DOI: 10.31510/infa.v23i1.2441.

LICENÇA

Artigo de acesso aberto distribuído sob a licença Creative Commons Atribuição 4.0 Internacional.

cc BY 4.0

RESUMO

Este artigo analisa a relação entre sustentabilidade energética e segurança da informação em data centers voltados à Inteligência Artificial (IA), investigando de que forma a escassez e a instabilidade no fornecimento de energia podem comprometer a continuidade operacional dessas infraestruturas críticas. O avanço da IA tem impulsionado a expansão de data centers de alto desempenho, intensificando significativamente a demanda por energia elétrica e introduzindo novos riscos à segurança da informação, especialmente no que se refere à disponibilidade dos serviços digitais. A pesquisa adota abordagem qualitativa e exploratória, fundamentada em revisão sistemática da literatura recente, seguindo os princípios do modelo PRISMA, com análise comparativa e de conteúdo de 20 estudos selecionados, considerando variáveis como redundância elétrica, uso de fontes renováveis e estratégias de eficiência térmica. Os resultados indicam que o aumento do consumo energético associado às cargas de trabalho em IA amplia a exposição a riscos de indisponibilidade, especialmente em regiões com infraestrutura elétrica limitada. Evidencia-se que a adoção integrada de práticas sustentáveis, como geração distribuída, reaproveitamento de calor e otimização de sistemas de refrigeração, contribui significativamente para a resiliência operacional e para a mitigação de riscos à segurança digital. Conclui-se que sustentabilidade energética e segurança da informação constituem dimensões interdependentes no projeto e na gestão de data centers contemporâneos, demandando abordagens sistêmicas que integrem eficiência energética, continuidade de negócios e proteção da informação.

Palavras-chave: Data centers. IA. Segurança da informação. Sustentabilidade. Disponibilidade.

ABSTRACT

This article analyzes the relationship between energy sustainability and information security in Artificial Intelligence (AI) oriented data centers, investigating how energy scarcity and supply instability may compromise the operational continuity of these critical infrastructures. The advancement of AI has driven the expansion of high-performance data centers, significantly increasing the demand for electrical energy and introducing new risks to information security, particularly with regard to the availability of digital services. The research adopts a qualitative and exploratory approach grounded in a systematic literature review following PRISMA principles, with comparative and

content analysis of 20 selected studies, considering variables such as electrical redundancy, the use of renewable energy sources, and thermal efficiency strategies. The results indicate that the increased energy consumption associated with AI workloads amplifies exposure to availability risks, especially in regions with limited electrical infrastructure. It is evidenced that the integrated adoption of sustainable practices, such as distributed generation, heat reuse, and optimization of cooling systems, significantly contributes to operational resilience and to the mitigation of risks to digital security. It is concluded that energy sustainability and information security constitute interdependent dimensions in the design and management of contemporary data centers, requiring systemic approaches that integrate energy efficiency, business continuity, and information protection.

Keywords: Data centers. Artificial intelligence. Information security. Sustainability. Availability.

1 INTRODUÇÃO

O avanço da IA tem acelerado transformações profundas na forma como as organizações processam, armazenam e analisam dados. Para sustentar esse ritmo, há uma crescente necessidade de ambientes computacionais mais potentes, como os *data centers* de alto desempenho, capazes de lidar com cargas intensivas de trabalho. Esses espaços concentram grandes volumes de equipamentos, operando continuamente para treinar modelos, processar dados e oferecer serviços em tempo real.

No entanto, toda essa capacidade exige grandes quantidades de energia. De acordo com a Agência Internacional de Energia (IEA, 2024), o consumo de eletricidade por *data centers* poderá ultrapassar 1.200 TWh até 2035, principalmente por conta do uso intensivo de IA. Esse número é comparável ao consumo total de energia de países inteiros e representa um alerta para os riscos de sobrecarga em redes locais e regionais.

Além do aumento da demanda energética, pesquisas também apontam que o treinamento de modelos avançados de IA pode exigir enormes quantidades de recursos computacionais e eletricidade, intensificando desafios relacionados à eficiência energética e à sustentabilidade digital (MIT TECHNOLOGY REVIEW, 2024; MCKINSEY & COMPANY, 2023). Como consequência, cresce a preocupação sobre a capacidade das infraestruturas elétricas de suportar essa expansão, especialmente em regiões onde a rede energética apresenta limitações estruturais.

Esse cenário não representa apenas um desafio ambiental ou econômico. A dependência direta da energia elétrica torna os *data centers* altamente sensíveis a instabilidades no fornecimento energético, o que pode impactar diretamente a continuidade dos serviços digitais. Falhas no suprimento elétrico podem provocar indisponibilidade de sistemas, interrupções de serviços em nuvem, perda de sessões e até corrupção de dados em processos em execução. Sob a perspectiva da segurança da informação, tais eventos afetam diretamente o princípio da disponibilidade, considerado um dos pilares fundamentais da proteção de sistemas e dados. De acordo com o National Institute of Standards and Technology (NIST), a disponibilidade garante que sistemas e informações permaneçam acessíveis e operacionais sempre que necessários (NIST, 2020). De forma semelhante, a norma ISO/IEC 27001 estabelece que a continuidade e a resiliência operacional são elementos essenciais para a proteção de ativos informacionais críticos (ISO/IEC, 2022).

Embora o consumo de *data centers* seja frequentemente debatido sob a ótica da sustentabilidade, há carência de pesquisas que o tratem como um risco direto à segurança da informação, visto que a dependência da infraestrutura para aplicações de IA amplia a exposição a indisponibilidades em cenários de sobrecarga ou instabilidade da rede (ENERGY-AWARE..., 2023). Em países como o Brasil, esse cenário é ainda mais crítico, pois a expansão acelerada para suportar a IA re-

vela gargalos estruturais na capacidade de fornecimento, comprometendo a estabilidade das infraestruturas digitais (EIXOS ENERGIA, 2026; CGI.BR, 2026).

Diante desse contexto, surge o seguinte problema: de que maneira a crescente demanda energética impulsionada pela IA, em conjunto com a escassez e instabilidade no fornecimento de energia, impacta a disponibilidade da informação em *data centers*, e como a adoção de práticas sustentáveis pode mitigar esses riscos, fortalecendo a resiliência operacional e a segurança digital?

Parte-se da hipótese de que a adoção e integração de práticas sustentáveis, como o uso de fontes de energia renováveis, a otimização de sistemas de refrigeração e o reaproveitamento de calor, em *data centers* que operam com IA, não apenas minimiza o impacto ambiental, mas também fortalece significativamente a resiliência operacional e a disponibilidade da informação, atuando como uma estratégia eficaz de mitigação contra os riscos emergentes da escassez e instabilidade energética.

O objetivo geral deste trabalho é analisar como a escassez e a instabilidade no fornecimento de energia impactam a disponibilidade da informação, avaliando de que forma a integração de práticas sustentáveis atua como uma estratégia de mitigação de riscos e fortalecimento da resiliência operacional. Essa investigação torna-se imperativa diante da projeção de que o consumo global de eletricidade por esses centros possa ultrapassar 1.200 TWh até 2035 (IEA, 2024) e considerando que a disponibilidade é um pilar fundamental da proteção de sistemas críticos (NIST, 2020).

2 REFERENCIAL TEÓRICO

A escassez de energia elétrica e a busca por eficiência nos *data centers* estão diretamente ligadas à forma como é tratada a Segurança da Informação em ambientes digitais. Para compreender essa relação, são abordadas neste capítulo três dimensões principais: a infraestrutura energética dos *data centers* voltados à IA, o papel da disponibilidade como pilar da segurança da informação e as práticas sustentáveis que contribuem para a resiliência dessas infraestruturas.

2.1 Infraestrutura e demanda energética dos data centers de IA

Os *data centers* que operam com IA são muito mais exigentes em termos de energia do que aqueles voltados a aplicações tradicionais. Isso acontece porque o treinamento e a execução de modelos de IA, como algoritmos de linguagem, visão computacional e análise preditiva, exigem processamento paralelo intenso, geralmente feito com GPUs, TPUs e servidores de alto desempenho. Essa demanda energética crescente é o cerne do problema investigado neste artigo, pois a sobrecarga na infraestrutura elétrica impacta diretamente a disponibilidade dos serviços.

Segundo a IEA (2024), um único *data center* de grande porte pode consumir energia equivalente a 100 mil residências. Os maiores projetos em desenvolvimento, como alguns nos Estados Unidos e na Europa, podem alcançar o consumo de 2 milhões de casas. Isso representa uma mudança significativa na relação entre tecnologia digital e infraestrutura energética, evidenciando a magnitude do desafio que pode comprometer a segurança da informação.

Além disso, o crescimento da IA tem levado à concentração de *data centers* em regiões específicas, como Virgínia (EUA), Irlanda e partes da Ásia, o que pressiona ainda mais a rede elétrica local. A McKinsey (2023) aponta que a energia já se tornou um dos principais limitadores físicos

para a expansão sustentável desses ambientes. Em regiões onde a rede elétrica não é resiliente, oscilações, quedas e cortes inesperados de energia podem interromper serviços essenciais, afetando empresas, governos e até setores críticos como saúde e transporte.

O Brasil conta atualmente com mais de 180 *data centers* operando, com projeções indicando a instalação de até 500 unidades até 2034, o que representaria uma demanda adicional de aproximadamente 2,5 GW de energia equivalente à capacidade de uma grande hidrelétrica. Esse crescimento ocorre em um cenário de infraestrutura elétrica assimétrica, com gargalos em regiões periféricas e limitações na integração de fontes renováveis (NEOFEED, 2025; EIXOS ENERGIA, 2026).

2.2 Disponibilidade como pilar da segurança da informação

Dentro da segurança da informação, um dos princípios mais importantes é a disponibilidade. Isso significa garantir que os dados e sistemas estejam acessíveis sempre que forem necessários, mesmo em situações adversas. Em ambientes de missão crítica, como os *data centers*, essa disponibilidade precisa ser garantida 24 horas por dia, todos os dias do ano.

A norma NIST SP 800-53 Rev. 5 (2020) trata a disponibilidade como um requisito básico para qualquer sistema seguro. No entanto, ela depende diretamente de condições físicas estáveis, sendo o fornecimento de energia elétrica uma delas. Falhas nesse fornecimento podem gerar impactos não apenas operacionais, mas também relacionados à confiança nos serviços e à proteção de dados.

Normas como a ISO/IEC 22301, voltadas à gestão da continuidade de negócios, destacam a importância de antecipar falhas de infraestrutura como parte da estratégia de segurança da informação. Em *data centers* de missão crítica, planos de *failover* automático, redundância geográfica e mecanismos de balanceamento de carga são exemplos de medidas técnicas que complementam o esforço por estabilidade energética.

2.3 Sustentabilidade e resiliência operacional

Arbache (2024) destaca que, embora os *data centers* representem oportunidades de inovação e desenvolvimento econômico, sua instalação pode gerar impactos ambientais e energéticos relevantes, especialmente quando não há planejamento adequado desde a concepção do projeto. O autor reforça a importância de incorporar critérios de sustentabilidade desde o início dos projetos, como demonstram iniciativas internacionais que reutilizam o calor gerado pelos servidores ou adotam exclusivamente energia renovável.

Exemplos internacionais, como o Equinix PA10 em Paris que durante os Jogos Olímpicos de 2024 reutilizou o calor gerado pelos servidores para aquecer piscinas públicas (DATACENTERDYNAMICS, 2024) e o *data center* do Google em Hamina, na Finlândia, que utiliza água do mar para resfriamento, demonstram que práticas sustentáveis podem transformar um problema ambiental em uma solução para a resiliência energética. Iniciativas semelhantes da Microsoft, AWS e Huawei também evidenciam que o uso de energias renováveis e arquiteturas eficientes pode reforçar a continuidade operacional e mitigar riscos.

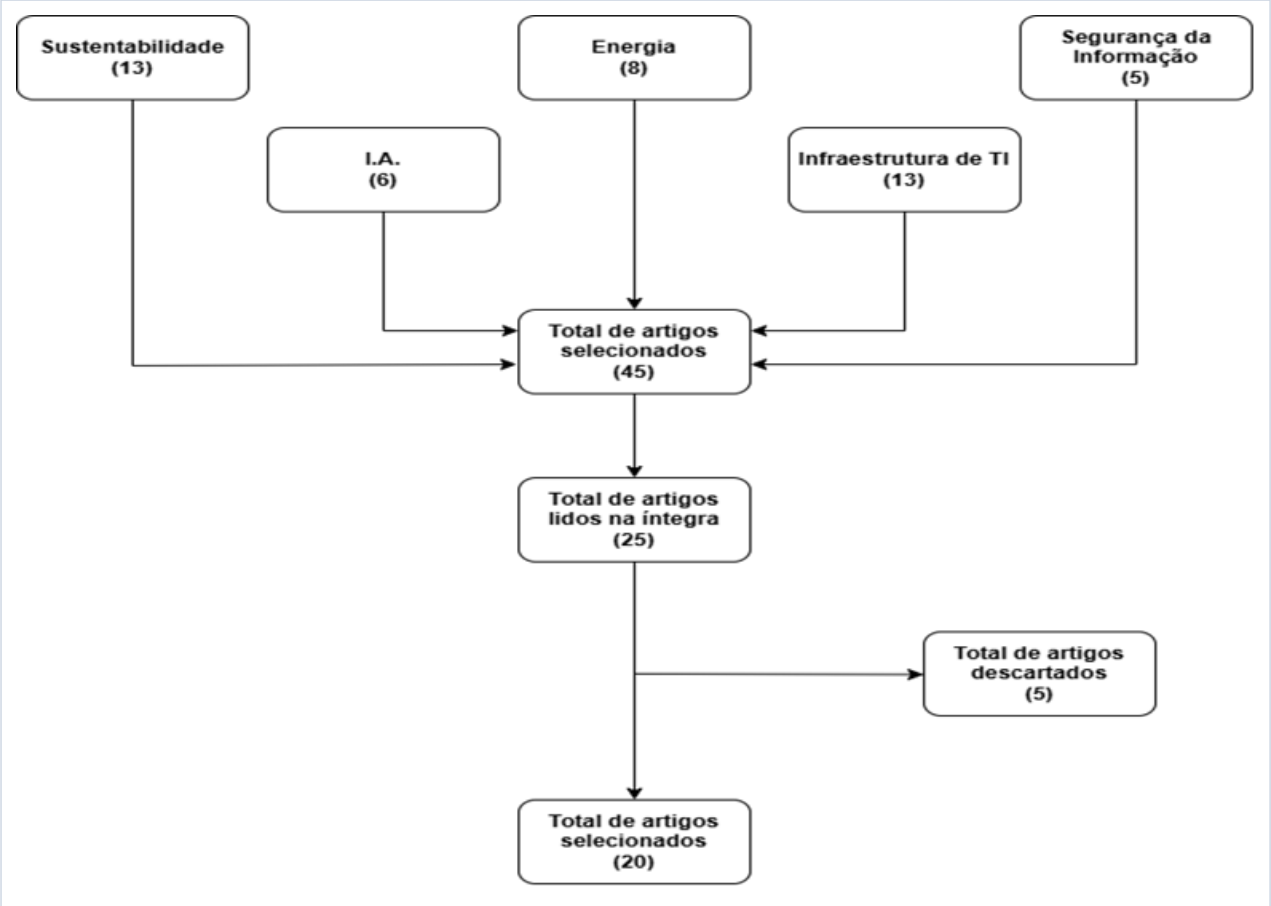
Assim, observa-se na literatura um ponto de convergência: a sustentabilidade não é apenas um imperativo ambiental, mas uma estratégia de mitigação de riscos energéticos. Esse entendimento conecta-se diretamente à hipótese deste artigo, que defende a adoção de práticas sustentáveis como forma de preservar a disponibilidade da informação em cenários de instabilidade energética.

3 METODOLOGIA

Este trabalho caracteriza-se como uma pesquisa bibliográfica de natureza qualitativa, com abordagem exploratória e descritiva, voltada à análise da relação entre escassez e instabilidade energética e os riscos para a segurança da informação em *data centers* que operam com Inteligência Artificial (IA), bem como ao papel das práticas sustentáveis na mitigação desses riscos. A pesquisa bibliográfica foi conduzida por meio de revisão de literatura em bases como IEEE Xplore, Scopus, ScienceDirect e Google Acadêmico, utilizando termos como "sustentabilidade em data centers", "infraestrutura de IA", "risco energético", "disponibilidade da informação", "resiliência energética" e "infraestrutura crítica". O recorte temporal considerou publicações entre 2020 e 2024, priorizando trabalhos em inglês e português.

O processo de seleção seguiu os princípios do modelo PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*). Inicialmente foram identificados 45 estudos relacionados aos temas da pesquisa, distribuídos nas categorias sustentabilidade (13), infraestrutura de TI (13), energia (8), inteligência artificial (6) e segurança da informação (5). Após leitura integral de 25 artigos, foram aplicados critérios de inclusão e exclusão, considerando relevância temática, aderência ao problema de pesquisa e atualidade das publicações. Foram excluídos 5 estudos por não abordarem diretamente a relação entre infraestrutura energética e segurança da informação em *data centers*. Ao final do processo, 20 artigos compuseram o *corpus* final de análise, conforme apresentado na Figura 1.

Figura 1 – Fluxograma PRISMA do processo de seleção dos artigos utilizados



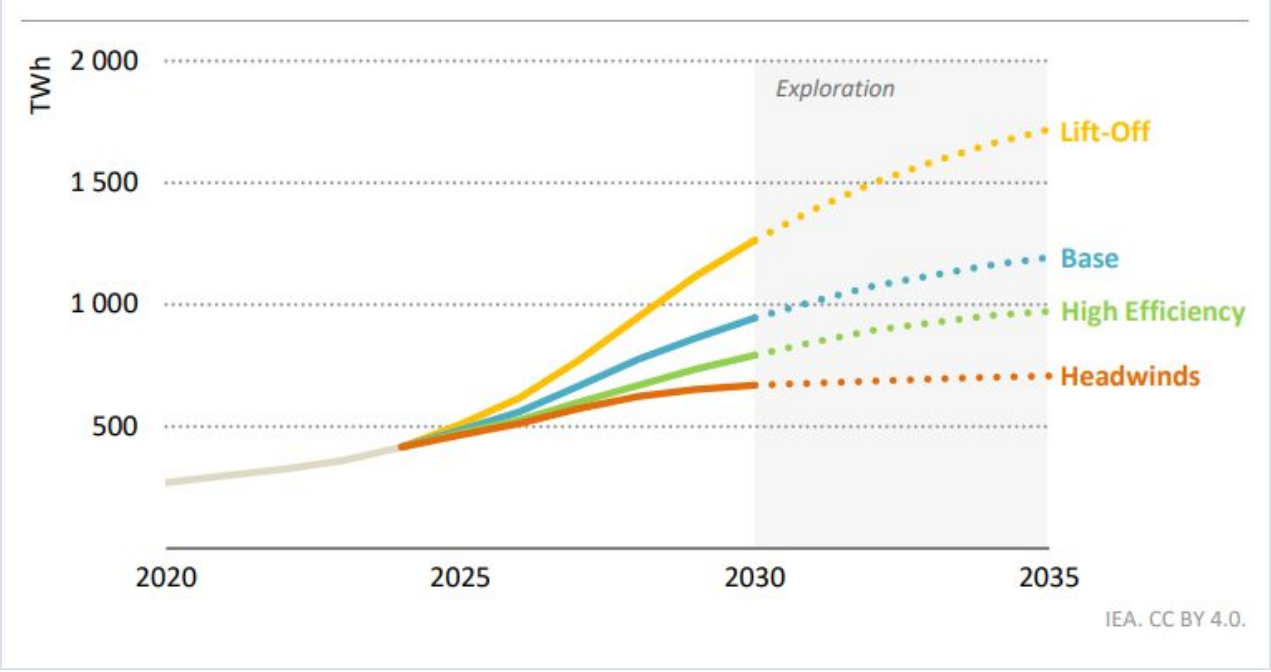
Fonte: Elaborado pelos autores (2025).

Os dados coletados foram analisados por meio de análise comparativa e análise de conteúdo, permitindo identificar convergências entre os estudos selecionados quanto aos riscos energéticos associados à operação de *data centers* e às estratégias adotadas para aumentar a resiliência dessas infraestruturas. Em uma etapa final, foi realizado um mapeamento de práticas sustentáveis aplicadas a *data centers*, incluindo iniciativas relacionadas à eficiência energética, uso de fontes renováveis e reaproveitamento térmico, avaliando seu potencial impacto sobre a segurança da informação e a resiliência operacional.

4 RESULTADOS E DISCUSSÃO

A análise dos 20 artigos selecionados permitiu identificar três pontos principais: o aumento da demanda de energia provocado pela IA, os impactos das falhas elétricas na disponibilidade dos serviços e o uso de práticas sustentáveis para reduzir esses riscos. No primeiro ponto, os estudos analisados mostram que o consumo de energia dos data centers deve crescer significativamente nos próximos anos. Segundo a Agência Internacional de Energia (IEA, 2025), a demanda global poderá atingir cerca de 1.200 TWh até 2035 no cenário base, podendo chegar a aproximadamente 1.200 TWh em cenários de maior expansão da IA, conforme apresentado na Figura 2. Apesar de diferenças entre os estudos sobre onde esse crescimento será mais intenso, muitos apontam que a concentração de data centers em determinadas regiões aumenta a pressão sobre a infraestrutura elétrica local. Além disso, observou-se que falhas na rede elétrica dessas regiões podem afetar diversos serviços ao mesmo tempo, ampliando os riscos de indisponibilidade.

Figura 2 – Projeção de consumo elétrico por data centers até 2035



Fonte: IEA (2024).

No segundo ponto, foi possível observar que poucos trabalhos abordam diretamente a relação entre instabilidade elétrica e disponibilidade da informação. Isso mostra que ainda existe espaço para novas pesquisas sobre o tema. Os casos do incêndio no data center da OVH (2021) e do alerta de sobrecarga na região de Ashburn (2023) demonstram que problemas na infraestrutura fí-

sica podem causar interrupções com impactos semelhantes aos de incidentes cibernéticos, conforme apresentado no Quadro 1.

Quadro 1 – **Marcos relevantes entre infraestrutura energética e segurança digital**

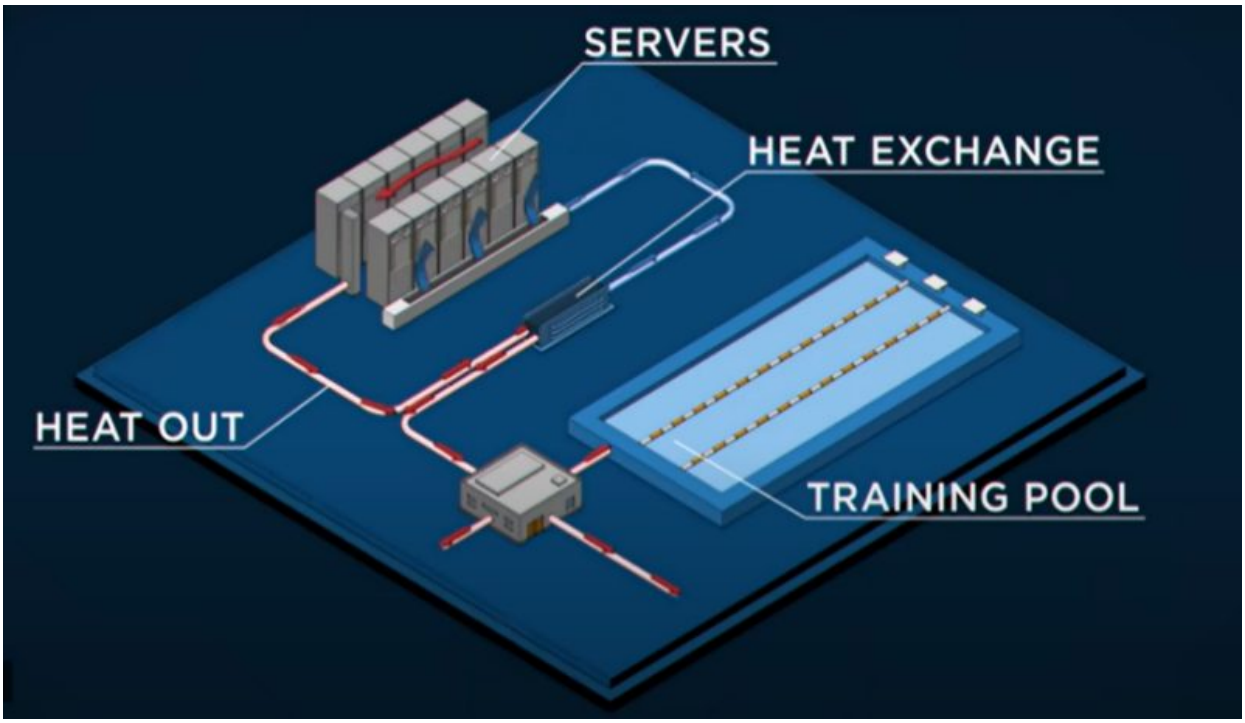
Ano	Evento	Impacto
2021	Incêndio no data center da OVH (França)	Queda de milhares de sites; perda de continuidade por falha elétrica.
2023	Alerta de sobrecarga em Ashburn (EUA)	Suspensão de licenças para novos data centers.
2025	Crescimento descontrolado de IA (cenário projetado)	Risco sistêmico de indisponibilidade em regiões críticas.

Fonte: Elaborado pelos autores (2025), com base em The Verge (2021) e The Washington Post (2023).

No terceiro ponto, a maior parte dos estudos destaca que práticas sustentáveis podem ajudar a reduzir os riscos de indisponibilidade. Entre as soluções mais citadas estão o reaproveitamento de calor, o resfriamento líquido e os sistemas de armazenamento de energia. O projeto Equinix PA10, apresentado na Figura 3, é um exemplo dessa abordagem, ao combinar eficiência energética e continuidade operacional. No Brasil, porém, desafios relacionados à infraestrutura elétrica e à regulamentação ainda dificultam a adoção dessas práticas em larga escala.

Além disso, a literatura aponta que o avanço da inteligência artificial tem impulsionado a evolução dos data centers para arquiteturas de maior densidade computacional e energética. Nesse cenário, tecnologias como o resfriamento líquido e os sistemas de armazenamento de energia por baterias (*Battery Energy Storage Systems*) ganham relevância para garantir a continuidade operacional e reduzir a dependência da rede elétrica. No contexto brasileiro, iniciativas recentes, como a Lei nº 15.269/2025 (EIXOS ENERGIA, 2026) e o programa Redata (CGI.BR, 2026), demonstram uma preocupação crescente com a expansão sustentável da infraestrutura digital, buscando estimular investimentos em data centers e fortalecer a capacidade energética necessária para suportar o crescimento da demanda.

Figura 3 – Projeto implementado pela Equinix nas Olimpíadas de Paris em 2024



Fonte: DatacenterDynamics (2024).

De forma geral, os resultados indicam que a resiliência dos data centers voltados à IA depende não apenas da capacidade de processamento, mas também de um planejamento energético adequado e de estratégias que garantam a continuidade dos serviços. Os estudos analisados também mostram que práticas sustentáveis podem contribuir para reduzir riscos operacionais e fortalecer a disponibilidade das informações.

5 CONSIDERAÇÕES FINAIS

Este estudo teve como objetivo analisar os impactos do crescimento da inteligência artificial sobre o consumo energético dos data centers, compreender a relação entre infraestrutura energética e disponibilidade da informação e avaliar práticas sustentáveis capazes de contribuir para a resiliência operacional dessas infraestruturas.

Os resultados obtidos demonstram que a expansão da IA impulsiona significativamente a demanda por energia elétrica, podendo elevar o consumo dos data centers para patamares superiores a 1.200 TWh até 2035. A análise dos estudos selecionados permitiu identificar que a infraestrutura energética se tornou um fator estratégico para a continuidade dos serviços digitais, uma vez que falhas no fornecimento elétrico podem gerar indisponibilidades com impactos comparáveis aos de incidentes cibernéticos.

Também foi possível verificar que práticas sustentáveis, como reaproveitamento térmico, resfriamento líquido, utilização de fontes renováveis e sistemas de armazenamento de energia, contribuem para aumentar a eficiência energética e reduzir riscos operacionais. Além disso, iniciativas regulatórias e programas de incentivo voltados à modernização da infraestrutura digital podem desempenhar papel relevante na expansão sustentável dos data centers.

Dessa forma, os objetivos propostos foram alcançados, evidenciando que a sustentabilidade não deve ser tratada apenas como uma questão ambiental, mas também como um elemento estratégico para a garantia da disponibilidade, continuidade e resiliência dos serviços de informação. Como sugestão para trabalhos futuros, recomenda-se o desenvolvimento de estudos voltados à aplicação de modelos preditivos e sistemas de monitoramento em tempo real capazes de antecipar falhas energéticas e apoiar a tomada de decisão em ambientes críticos.

REFERÊNCIAS

AI WORKLOADS and their impact on future data center design. **IEEE Access**, [*s. l.*], 2022. DOI: https://doi.org/10.1109/ACCESS.2022.3181623. Disponível em: https://ieeexplore.ieee.org/document/9872589. Acesso em: 5 jun. 2025.

ALVES, Raoni. US$ 65 bilhões em *data centers*: saiba mais sobre Rio AI City. **G1 Rio**, Rio de Janeiro, 2025. Disponível em: https://g1.globo.com/rj/rio-de-janeiro. Acesso em: 8 mar. 2026.

AMAZON WEB SERVICES. **Sustainability in the cloud**. Seattle: AWS, 2023. Disponível em: https://aws.amazon.com/sustainability/. Acesso em: 5 jun. 2025.

ARBACHE, Jorge. **Os custos e benefícios dos *data centers***. Rio de Janeiro: Grupo de Estudos do Setor Elétrico (GESEL/UFRJ), 2024. Disponível em: https://gesel.ie.ufrj.br/wp-content/uploads/2024/11/Sobre-os-beneficios-dos-data-centers-Jorge-Arbache_VF.pdf. Acesso em: 5 jun. 2025.

BEZERRA, Thiago Valentim. **Uma estratégia baseada em modelos para a quantificação do impacto da disponibilidade no fluxo energético de data centers**. 2019. Dissertação (Mestrado em Informática Aplicada) – Universidade Federal Rural de Pernambuco, Recife, 2019. Disponível em: http://callou.pythonanywhere.com/static/pdf/Dissertacao2019Thiago.pdf. Acesso em: 8 mar. 2026.

CGI.BR – COMITÊ GESTOR DA INTERNET NO BRASIL. **A corrida do Brasil por poder computacional**. São Paulo: CGI.br, 2026. Disponível em: https://cgi.br/publicacoes/revista-br/. Acesso em: 8 mar. 2026.

DATACENTERDYNAMICS. Equinix Paris *data center* to heat Olympic pools in 2024. **DatacenterDynamics**, Londres, 2024. Disponível em: https://www.datacenterdynamics.com/en/news/equinix-paris-data-center-to-heat-olympic-pools-in-2024/. Acesso em: 1 jun. 2025.

EIXOS ENERGIA. *Data centers* avançam e revelam gargalos críticos da infraestrutura brasileira. **Eixos Energia**, 2026. Disponível em: https://eixos.com.br/energia-eletrica/data-centers-avancam-e-revelam-gargalos-criticos-da-infraestrutura-brasileira. Acesso em: 11 mar. 2026.

ENERGY-AWARE cloud computing and security implications. **Journal of Information Security and Applications**, Amsterdam, v. 75, 2023. DOI: https://doi.org/10.1016/j.jisa.2023.103376. Disponível em: https://www.sciencedirect.com/science/article/pii/S2214212623000754. Acesso em: 5 jun. 2025.

FRANÇA, V. **Desafios energéticos em treinamento de modelos de inteligência artificial**. 2023. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – Pontifícia Universidade Católica de Goiás, Goiânia, 2023. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/7901. Acesso em: 5 jun. 2025.

IEA – INTERNATIONAL ENERGY AGENCY. AI is set to drive surging electricity demand from *data centres*. **IEA**, Paris, 2024. Disponível em: https://www.iea.org/news/ai-is-set-to-drive-surging-electricity-demand-from-data-centres. Acesso em: 5 jun. 2025.

ISO/IEC – INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 22301:2019**: security and resilience: business continuity management systems: requirements. Genebra: ISO, 2019.

ISO/IEC – INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27001:2022**: information security, cybersecurity and privacy protection: information security management systems: requirements. Genebra: ISO, 2022.

MCKINSEY & COMPANY. How *data centers* and the energy sector can sate AI's hunger for power. **McKinsey & Company**, Nova York, 2023. Disponível em: https://www.mckinsey.com/industries/electric-power-and-natural-gas/our-insights/how-data-centers-and-the-energy-sector-can-sate-ais-hunger-for-power. Acesso em: 1 jun. 2025.

MIT TECHNOLOGY REVIEW. The hidden energy cost of artificial intelligence. **MIT Technology Review**, Cambridge, 2024. Disponível em: https://www.technologyreview.com/2024/03/13/1089335/the-hidden-energy-cost-of-artificial-intelligence/. Acesso em: 5 jun. 2025.

NEOFEED. No plano trilionário de *data centers* do governo federal pode faltar energia, literalmente. **Neofeed**, São Paulo, 2025. Disponível em: https://neofeed.com.br/poder/no-plano-trilionario-de-data-centers-do-governo-federal-pode-faltar-energia-literalmente/. Acesso em: 8 mar. 2026.

NIST – NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **SP 800-53 Rev. 5**: security and privacy controls for information systems and organizations. Gaithersburg: NIST, 2020. Disponível em: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final. Acesso em: 31 maio 2025.

SCIENTIFIC AMERICAN. The AI boom could use a shocking amount of electricity. **Scientific American**, Nova York, 2024. Disponível em: https://www.scientificamerican.com/article/the-ai-boom-could-use-a-shocking-amount-of-electricity/. Acesso em: 5 jun. 2025.

SECURITY COMPASS. Availability in cloud security architecture. **Security Compass**, Toronto, 2024. Disponível em: https://www.securitycompass.com/resources/cloud-architecture-availability/. Acesso em: 31 maio 2025.

WORLD ECONOMIC FORUM. Digital infrastructure and net-zero emissions. **World Economic Forum**, Genebra, 2023. Disponível em: https://www.weforum.org/reports/digital-infrastructure-and-net-zero-emissions/. Acesso em: 5 jun. 2025.

Os conceitos e as opiniões expressos neste artigo são de responsabilidade exclusiva de seus autores.