WESTERN HEMISPHERE READINESS SERIES

HRS RESILIENCE FOUNDATION

SECTOR READINESS ASSESSMENT 02

Data Centers, Cloud & AI Infrastructure

Energy, Continuity, Security and Strategic Dependency

PUBLICATION TYPE	PRIMARY ENVIRONMENT	EDITION
Independent sector readiness assessment	Brazil, with Western Hemisphere applicability	August 2026

SERIES POSITION	AUTHOR	INSTITUTION
Sector Readiness Assessment 02	André Vieira	HRS Resilience Foundation

CONTENTS

About this series. The Western Hemisphere Readiness Series applies the HRS Readiness Cycle — Detect, Assess, Decide, Coordinate, Deploy, Sustain, Learn — to critical sectors across the Americas. Sector Readiness Assessment 02 is the sixth publication in the HRS Resilience Foundation's body of original research, following Strategic Report 01, Policy Brief 01, Technical Paper 01, Country Readiness Assessment 01 — Brazil, and Sector Readiness Assessment 01 — Telecommunications & Digital Infrastructure.

EXECUTIVE SUMMARY

Data Centers, Cloud & AI Infrastructure

Data centers are becoming foundational infrastructure for cloud services, artificial intelligence, scientific computing, digital government, communications, finance, healthcare and other critical functions.

The HRS framework treats the data center as a system node rather than an isolated building. Readiness depends on electricity, transmission, telecommunications, cooling, hardware, software, cloud architecture, cybersecurity, physical security, workforce and recovery capability.

NIST's July 2026 draft SP 800-239 identifies AI data centers as a distinct high-performance-computing security environment, with important differences across architecture, hardware, software, workflows and storage. DOE's 2026 draft National Transmission Needs Study identifies hyperscale AI data centers as a major source of load growth and emphasizes reliable and secure grid expansion. Brazil's EPE likewise identifies data centers as large loads affecting transmission planning.

HRS CENTRAL PROPOSITION

AI readiness is infrastructure readiness. Compute capacity without dependable energy, connectivity, security, supply chains and recovery capability is not operational readiness.

HRS treats national sovereignty over infrastructure, technology, and international-partnership decisions as a foundational premise of this methodology, not a variable to be assessed. The purpose of this assessment is to strengthen the capacity of sovereign institutions to identify their own exposures and expand their own range of options — never to prescribe which supplier, technology, or foreign partner a country should choose.

SECTION 01

Purpose and Scope

This assessment extends the HRS Readiness Cycle into the computing layer that increasingly powers cloud and AI services.

It covers conventional enterprise and hyperscale data centers, cloud infrastructure, high-performance computing and AI-oriented facilities.

> *Can data-center, cloud and AI infrastructure sustain essential computing functions when exposed to energy constraints, connectivity disruption, cyber incidents, equipment or supply-chain disruption, physical events, workforce limitations or loss of a critical provider?*

This is a public-source sector readiness assessment — not a classified intelligence estimate, engineering audit, legal opinion or certification.

Foreign ownership or technology is not treated as inherently harmful. The assessment focuses on dependency, control, substitutability, security and recovery.

SECTION 02

Why Data Centers Have Become Strategic Infrastructure

NTIA states that data centers enable cloud services and cutting-edge AI technologies and that their growth must be balanced with data security and resilient supply chains. This creates a structural transformation: computing is increasingly an infrastructure dependency.

Energy → Data Center → Compute → Cloud / AI → Digital Services → Critical Functions

Data centers also depend upon telecommunications, power, cooling, trusted equipment, software, skilled personnel, physical security and recovery systems.

The strategic question is not simply how large a data center is. It is how many critical functions depend upon it and how quickly those functions can be maintained or restored if the facility or one of its dependencies fails.

SECTION 03

The HRS Data Center Readiness Cycle

FUNCTION	READINESS TASK
Detect	Identify degradation in power, cooling, connectivity, security, hardware, software or supply chains.
Assess	Convert technical telemetry into a credible operational picture.
Decide	Establish escalation thresholds, shutdown priorities and restoration decisions.
Coordinate	Synchronize facility, utility, network, cloud, security and government stakeholders.
Deploy	Activate alternate power, connectivity, compute, equipment and personnel.
Sustain	Maintain essential workloads during prolonged degradation.
Learn	Convert incidents and exercises into measurable architectural and operational improvements.

> *The HRS principle remains: a dependency does not prove failure. The relevant question is whether it is understood, governed, monitored and recoverable.*

SECTION 04

Energy, Power and Grid Dependency

Energy is the defining physical dependency of large-scale computing.

NTIA reported that U.S. data centers consumed more than four percent of total U.S. electricity in 2022 and cited projections that the share could reach up to nine percent by 2030. DOE's 2026 draft National Transmission Needs Study identifies rapid load growth from hyperscale AI data centers and states that the grid must expand while remaining reliable and secure.

Brazil's EPE states that data centers are large loads whose power demand directly affects transmission-expansion planning and that their accelerated growth is increasing local and regional load.

HRS Power Readiness Questions

- Is primary supply sufficiently reliable for the workload?
- Are backup pathways genuinely independent?
- Can backup systems operate for the required duration?
- Can fuel, maintenance and replacement components be sustained?
- Is interconnection capacity sufficient for planned expansion?
- Could regional grid stress affect primary and backup arrangements?
- Are power-restoration priorities integrated with data-center recovery?

SECTION 05

Cooling, Water and Thermal Resilience

High-density computing creates substantial thermal-management requirements. Cooling therefore belongs inside the readiness model rather than being treated as a facilities-management detail.

The appropriate cooling strategy varies by architecture, climate, workload, facility design and technology. HRS does not prescribe a single technology; it evaluates whether thermal management remains available during disruption.

Where water is part of the cooling architecture, water availability and local infrastructure should be treated as dependencies. Where alternative cooling architectures are used, their electricity and equipment dependencies must be assessed.

Thermal Readiness Questions

- Can cooling continue during electrical degradation?
- Are cooling components genuinely redundant?
- Can critical workloads be reduced or relocated before thermal failure?
- Can cooling equipment be repaired with available parts and personnel?
- Are water and other utility dependencies understood?
- Can thermal degradation be detected early enough to prevent service interruption?

SECTION 06

AI Infrastructure as a Distinct Readiness Environment

AI data centers differ from conventional environments because they are designed around high-performance computing architectures, specialized accelerators, large-scale storage and networking, model-training workflows and inference workloads.

NIST's initial public draft SP 800-239, published July 27, 2026, examines AI data-center security by comparing AI infrastructure with traditional HPC across architecture, hardware, software stacks, workflows and storage.

AI Readiness Dimensions

- **Accelerator dependency** — availability and replaceability of specialized compute hardware.
- **Interconnect dependency** — high-performance networking between compute nodes.
- **Storage** — integrity, availability, replication and recovery of large datasets and model artifacts.
- **Model weights** — protection, integrity, backup and controlled recovery of trained models.
- **Software stack** — drivers, orchestration, libraries, firmware and update mechanisms.
- **Workload continuity** — ability to move, pause, degrade or restore training and inference.
- **Security** — protection of hardware, software, data, model artifacts and administrative interfaces.

SECTION 07

Cloud Infrastructure and Multi-Cloud Continuity

Cloud architecture can improve resilience by distributing workloads and reducing dependence on a single physical facility. It can also create new complexity and dependency.

NIST's August 2026 initial public draft IR 8613 identifies multi-cloud challenges involving security-significant differences between providers, organizational complexity and difficulty implementing centralized security across provider boundaries. It highlights identity and access management, telemetry and logging, configuration and change management, data protection and authorization.

HRS CONCLUSION

Multi-cloud is not automatically resilient. Resilience depends on whether workloads can actually be moved, whether data can be recovered, whether security controls remain effective across providers and whether personnel can operate the architecture during disruption.

Cloud Dependency Test

- Portability
- Data portability
- Identity portability
- Observability
- Security continuity
- Workforce capability
- Cost and time to activate alternatives

SECTION 08

Cyber, Physical and Supply-Chain Security

Data-center security is multidimensional. NTIA identifies trusted ICTS equipment, supply-chain resilience, workforce and data security among the factors relevant to secure data-center growth.

AI environments amplify this challenge because specialized hardware, firmware, software stacks, model weights, storage systems and administrative interfaces create additional security-relevant dependencies. NIST's SP 800-239 draft provides an emerging technical basis for analyzing these environments.

HRS Security Domains

- **Physical** — facilities, access control, environmental systems and personnel safety.
- **Cyber** — networks, identity, endpoints, orchestration, logging and incident response.
- **Supply chain** — hardware, semiconductors, networking, firmware, software and maintenance.
- **Data** — confidentiality, integrity, availability, backup and recovery.
- **AI assets** — model weights, training pipelines, inference systems and specialized infrastructure.
- **Workforce** — trusted personnel, skills, staffing depth and continuity.

SECTION 09

Strategic Dependency and Concentration

The concentration of compute, cloud services, hardware, power, connectivity or technical expertise can create dependencies that are difficult to replace.

The HRS Strategic Dependency Test

QUESTION	WHAT IT EXAMINES
1. Concentration	How much essential capacity depends on one provider, facility, region, technology or supplier?
2. Substitutability	Can the dependency be replaced within an operationally acceptable period?
3. Control	Does the organization possess sufficient visibility, authority and access?
4. Recovery	Can essential services be restored without the failed dependency?
5. Cascading Impact	What other sectors, services or institutions depend upon the affected capability?

> *HRS deliberately avoids treating nationality as a substitute for evidence. A domestic dependency can be strategically significant; a foreign dependency may be manageable if it is transparent, replaceable, governed and recoverable.*

SECTION 10

Nominal Redundancy vs. Effective Redundancy

A recurring error in infrastructure planning is to count alternatives without testing whether they are truly independent.

CONCEPT	DEFINITION
Nominal redundancy	An apparent alternative exists.
Effective redundancy	The alternative can operate when the principal dependency fails.

For data centers this applies to power feeds and generators, network carriers and physical routes, cloud providers, compute hardware, geographic recovery sites, and cooling systems.

- **Power** — two feeds are not enough if both depend on the same failure path.
- **Connectivity** — two carriers are not enough if both use the same physical corridor.
- **Cloud** — two providers are not enough if workloads and data cannot actually move.
- **Compute** — spare servers are not enough if replacement hardware cannot support the workload.
- **Facilities** — two sites are not enough if both depend on the same regional infrastructure.

HRS PROPOSITION

More infrastructure does not automatically produce more resilience. Independence matters.

SECTION 11

Continuity, Recovery and Graceful Degradation

Not every workload requires identical continuity. Readiness improves when organizations classify workloads according to mission importance and define acceptable degradation and recovery conditions.

CLASS	CONTINUITY STANDARD
Essential	Maintain or rapidly restore.
Mission-critical	Minimize interruption through failover or rapid recovery.
Important	Recover within the planned period.
Deferrable	Accept controlled delay without damaging essential functions.

Graceful degradation should be designed before failure occurs. A system that can reduce nonessential workloads to preserve essential functions may be more resilient than a system designed around uninterrupted operation of every workload.

SECTION 12

Western Hemisphere Readiness

Data-center expansion is increasingly connected to national competitiveness, digital sovereignty, telecommunications resilience, energy planning, AI capability and critical infrastructure.

DOE describes data centers as enabling AI advances, scientific discovery, critical services, economic growth and national-security applications, and states that U.S. AI leadership requires energy infrastructure, computing capacity and skilled workforce development.

For the Western Hemisphere, the HRS question is not whether every country should reproduce the same infrastructure model. It is whether critical digital capabilities can remain available and recoverable as demand grows and technology changes.

Consistent with the HRS methodology, references to other governments' or institutions' strategic priorities are presented here as documented positioning, not as an HRS judgment on any country's technology or partnership choices. Decisions about vendors, energy strategy, and computing architecture remain the sovereign prerogative of each national government; the role of this assessment is to inform that decision-making capacity with evidence.

HRS PROPOSITION

Resilient national computing infrastructure contributes to resilient hemispheric digital infrastructure.

SECTION 13

HRS Data Center & AI Resilience Improvement Framework

1. Map Critical Dependencies — Identify power, transmission, connectivity, cooling, hardware, software, cloud, workforce and recovery dependencies.
2. Classify Critical Workloads — Define essential, mission-critical, important and deferrable functions.
3. Test Effective Redundancy — Verify that alternative power, network, cloud and facility paths are independently operable.
4. Establish Energy Readiness — Integrate data-center expansion with generation, transmission, interconnection and backup planning.
5. Protect AI-Specific Assets — Include accelerators, firmware, model weights, training pipelines and high-performance interconnects in security and recovery planning.
6. Build Cloud Portability — Validate that critical workloads and data can move between environments within an acceptable time.
7. Strengthen Supply-Chain Resilience — Assess semiconductor, networking, storage, power, cooling and maintenance dependencies.
8. Develop Workforce Depth — Maintain sufficient technical personnel and cross-training for prolonged disruption.
9. Exercise Degraded Operations — Test power loss, connectivity loss, cyber incidents, cooling failure, equipment shortage and provider unavailability.
10. Convert Lessons into Investment — Require after-action findings to change architecture, procurement, training and recovery plans.

SECTION 14

Long-Horizon Infrastructure Readiness

Data-center and AI infrastructure decisions can create dependencies for decades. Hardware generations change rapidly, but facilities, power interconnections, fiber routes, land, cooling systems, contracts, workforce structures and institutional arrangements may persist.

HRS therefore recommends designing for adaptability rather than optimizing only for current technology.

- Do not design critical capacity around a single irreversible dependency.
- Preserve the ability to replace hardware, software, cloud services and network providers.
- Integrate energy planning with compute expansion from the beginning.
- Maintain geographic diversity for workloads whose disruption would create material consequences.
- Require recovery exercises before declaring a system resilient.
- Build institutional knowledge that survives changes in vendors and administrations.

HRS INSTITUTIONAL DESIGN PRINCIPLE

HRS builds its readiness frameworks for a 50-year application horizon. Compute hardware will be replaced many times over that horizon; the institutions, energy planning, and decision-making capacity built around it should not need to be rebuilt with each generation. A framework designed only for the current technology cycle or the current administration is not a resilience framework — it is a temporary arrangement. The objective is not technological permanence. It is institutional and operational adaptability, so that sovereign institutions — not any single vendor or foreign relationship — remain in control of their own resilience over time.

SECTION 15

Conclusion

Data centers, cloud platforms and AI infrastructure are becoming a foundational layer of modern economic, institutional, scientific and security capability.

Their readiness cannot be measured by computing capacity alone. The decisive question is whether that capacity can remain available, secure, connected, powered, supported and recoverable when conditions deteriorate.

The HRS assessment identifies energy, connectivity, cooling, computing hardware, cloud architecture, cybersecurity, physical security, supply chains, workforce and recovery as a single readiness system.

CENTRAL CONCLUSION

AI infrastructure is only as resilient as the infrastructure that enables it.

Detect → Assess → Decide → Coordinate → Deploy → Sustain → Learn

The strategic objective is not simply to build more compute. It is to build compute capacity that can endure, adapt, recover and remain useful as technology and strategic conditions change.

METHODOLOGY, RESEARCH INTEGRITY AND LIMITATIONS

Methodology, Research Integrity and Limitations

This report is an original HRS Resilience Foundation synthesis based primarily on official U.S. and Brazilian government materials. Official sources establish factual claims about infrastructure, policy, regulatory developments and technical frameworks. The HRS Sector Readiness Profile, Strategic Dependency Test, Nominal-versus-Effective Redundancy framework and Data Center & AI Resilience Improvement Framework are original analytical constructs.

The report uses public information only. It does not claim access to classified intelligence or confidential operator information. Where evidence is insufficient to establish a current condition, the report frames the issue as a readiness question rather than a factual allegation.

No conclusion concerning a specific company, government, supplier, political party or individual should be inferred from sector-level analysis. Operational decisions require competent authorities, evidence, applicable law and appropriate due process.

This document is a public-source sector readiness assessment, not a security certification, engineering audit, legal opinion, procurement recommendation or classified threat assessment.

Research Integrity

- Documented fact is grounded in authoritative source material.
- Analytical judgment is presented as HRS assessment rather than external fact.
- Scenario reasoning is not presented as evidence of current conditions.
- Sector exposure is not equated with criminality or malign intent.
- Foreign participation is evaluated through dependency and resilience criteria rather than nationality alone.
- Sovereignty is a starting premise, not a variable: dependency analysis exists to expand the range of options available to national decision-makers, not to prescribe outcomes.

SELECTED BIBLIOGRAPHY AND SOURCES

Sources

[1] National Telecommunications and Information Administration (NTIA). Digital Infrastructure Resilience; Request for Comments on Bolstering Data Center Growth, Resilience, and Security. U.S. Department of Commerce.

[2] National Institute of Standards and Technology (NIST). SP 800-239, AI Data Center Security Analysis: A High-Performance Computing (HPC) Driven Approach. Initial Public Draft, July 27, 2026.

[3] U.S. Department of Energy, Office of Electricity. 2026 National Transmission Needs Study. Draft released July 9, 2026.

[4] Empresa de Pesquisa Energética (EPE), Brazil. Consumo de Energia Elétrica de Data Centers. Official energy-planning material.

[5] NIST. IR 8613, Multi-Cloud Architecture Challenges: Security and Compliance Implications. Initial Public Draft, August 21, 2026.

[6] U.S. Department of Energy. Powering America's AI Future — Data Center Resource Hub. 2026.

[7] NIST. Concept Note: AI Risk Management Framework Profile on Trustworthy AI in Critical Infrastructure. April 7, 2026.

[8] U.S. Department of Energy, Office of Electricity. Speed to Power Initiative — Accelerating Grid Capacity for AI and Large-Load Growth. Launched September 18, 2025; SPARK funding opportunity announced March 12, 2026.

[9] The White House. Executive Order 14262 — Strengthening the Reliability and Security of the United States Electric Grid. April 8, 2025; and subsequent DOE reliability and AI-infrastructure actions, 2025–2026.

[10] HRS Resilience Foundation. Strategic Report 01 — Health Security and Institutional Resilience in the Americas: From Preparedness to Operational Readiness. August 2026.

[11] HRS Resilience Foundation. Policy Brief 01 — Strengthening Regional Health Emergency Readiness in the Americas: From Early Warning to Action. August 2026.

[12] HRS Resilience Foundation. Technical Paper 01 — Building Resilient Health Supply Chains. August 2026.

[13] HRS Resilience Foundation. Country Readiness Assessment 01 — Brazil: Institutional Readiness, Critical Infrastructure and Health-Security Continuity. August 2026.

[14] HRS Resilience Foundation. Sector Readiness Assessment 01 — Telecommunications & Digital Infrastructure: Sector Readiness, Continuity and Strategic Dependency. August 2026.

Suggested citation: HRS Resilience Foundation. *Sector Readiness Assessment 02 — Data Centers, Cloud & AI Infrastructure: Energy, Continuity, Security and Strategic Dependency.* Western Hemisphere Readiness Series. August 2026.

WESTERN HEMISPHERE READINESS SERIES

HRS Resilience Foundation

Independent research for institutional readiness, continuity, and 50-year resilience planning across the Western Hemisphere. The Western Hemisphere Readiness Series applies the HRS Readiness Cycle to critical sectors, translating public-source evidence into practical frameworks built to remain valid for governments, infrastructure operators, investors, and institutional decision-makers across changes in technology, suppliers, and political leadership.

SERIES TO DATE

SRA 01 — Telecommunications & Digital Infrastructure
SRA 02 — Data Centers, Cloud & AI Infrastructure
SRA 03 — Critical Minerals & Strategic Materials
SRA 04 — Rare Earths & Western Hemisphere Mineral Security
SRA 05 — Energy Security & Strategic Power Infrastructure
SRA 06 — Ports, Logistics & Maritime Infrastructure
SRA 07 — Food Security & Strategic Agricultural Resilience
SRA 08 — Pharmaceutical & Medical Supply Chains
SRA 09 — Advanced Manufacturing & Industrial Capacity
SRA 10 — Western Hemisphere Strategic Infrastructure & Resilience

André Vieira, MD

FOUNDER & CHAIRMAN, HRS RESILIENCE FOUNDATION