Submitted March 3, 2026

CCIA Comments on ANATEL's Public Consultation No. 48

The Computer & Communications Industry Association (CCIA) respectfully submits the following comments in response to Brazil's National Telecommunications Agency (ANATEL) Public Consultation No. 48, which proposes to establish technical requirements and conformity assessment procedures for data centers integrated with telecommunications networks pursuant to Resolution No. 780 (2025).[1]

CCIA is an international, nonprofit trade association representing a broad cross section of communications and technology companies.[2] CCIA appreciates the opportunity to provide input on the proposed rule and offers the following comments for ANATEL's consideration.

Industry Concerns

CCIA respectfully recommends that ANATEL narrow the scope of this implementing decree to infrastructure that is structurally and functionally integrated into the core operation of licensed telecommunications networks. ANATEL should ensure that the scope clearly prevents facilities that only incidentally or indirectly process telecommunications data from being incorporated into the regulatory framework without proper technical assessment, while also making clear that regulatory responsibility and direct liability remain with licensed providers of telecommunications services of collective interest under the General Telecommunications Law.

As currently framed, the broad functional criteria risk sweeping general-purpose cloud and data center providers into scope even where they act solely as sector-agnostic third-party vendors supporting ancillary services and functions and do not control signaling, routing, switching, or traffic management functions.

A balanced, clearly targeted approach will better advance service resilience while supporting Brazil's objective of attracting and scaling data center investment.[3]

Section-specific feedback is as follows.

[1] ANATEL. (2026). *CONSULTA PÚBLICA Nº 48*. https://apps.anatel.gov.br/ParticipaAnatel/VisualizarTextoConsulta.aspx?TelaDeOrigem=2&ConsultaId=20370.

[2] For more, see https://ccianet.org/.

[3] CCIA. (2025) *CCIA Comments on Brazil National Data Center Policy "Connectivity and Infrastructure Axis."* https://ccianet.org/wp-content/uploads/2025/09/CCIA-Comments-on-Brazil-National-Data-Center-Policy.pdf.

Objectives

Section 1.1 states that the Draft establishes technical requirements and procedures for assessing the conformity of data centers that are part of telecommunications networks, under Title VI-A of the RACHPT as amended by Resolution No. 780/2025.[4]

As drafted, the objective does not clearly attribute regulatory responsibility to licensed telecommunications providers, as required under the General Telecommunications Law (LGT), which assigns primary and non-delegable responsibility for service quality, continuity, and security to telecom operators.[5] By framing the measure as applying to "data centers that are part of telecommunications networks," without clarifying who bears legal responsibility for compliance, the Draft creates ambiguity as to whether ANATEL intends to regulate operators' use of infrastructure or to impose direct obligations on data centers and other third-party digital infrastructure outside its statutory remit. Compliance with the regulation should be managed exclusively by the regulated operator, whether in relation to infrastructure it owns, operates, or controls, or, where applicable, through contractual arrangements with third-party vendors.

Section 1 should be revised to make explicit that licensed telecommunications providers remain fully responsible for compliance with ANATEL's service quality, continuity, and security obligations, including when they rely on third-party infrastructure. The Draft should clarify that the conformity assessment framework applies to telecommunications providers' use of infrastructure, rather than imposing direct regulatory obligations on non-telecommunications data center operators. This approach respects the distinct roles of telecommunications operators who manage public networks as opposed to third-party infrastructure providers offering shared services used by a broad range of industries, and who do not operate public telecommunications networks or provide telecommunication services to end users.

Current Text	Proposed Text
1. PURPOSE *1.1. This document establishes the technical requirements and operational procedure for the conformity assessment of data centers that are part of telecommunications networks, in compliance with the provisions contained in Title VI-A of the Regulation on Conformity Assessment and Approval of Telecommunications Products (RACHPT), approved by Resolution No. 715 of October 23, 2019, and amended by Anatel Resolution No. 780 of August 1, 2025.*	*1. PURPOSE* *1.1. This document establishes the technical requirements and operational procedure* ***applicable to licensed telecommunications service providers of collective interest (common carriers)*** *for the conformity assessment of data centers that are part of telecommunications networks, in compliance with the provisions contained in Title VI-A of the Regulation on Conformity Assessment and Approval of Telecommunications Products (RACHPT), approved by Resolution No. 715 of October 23,*

[4] *Resolução Anatel nº 780* [Brazil]. (2025). https://informacoes.anatel.gov.br/legislacao/component/content/article/170-resolucoes/2025/2054-resolucao-anatel-780.

[5] *LEI Nº 9.472* [Brazil]. (1997). https://www.planalto.gov.br/ccivil_03/LEIS/L9472.htm.

	2019, and amended by Anatel Resolution No. 780 of August 1, 2025. ***1.2 For the avoidance of doubt, licensed telecommunications service providers of collective interest (common carriers) remain fully and non-delegably responsible for compliance with all service quality, continuity, and security obligations established by ANATEL, including where such providers contract, use, or rely upon third-party infrastructure.*** ***1.3. The use of third-party infrastructure providers by a licensed telecommunications provider shall not, by itself, subject the third-party provider to direct regulatory obligations, inspection, certification requirements, or enforcement by ANATEL.***

Scope and Definitions

Under **Articles 3.1.1–3.1.3**, the draft implementing regulations are scoped to include infrastructure that is part of telecommunications networks and performs core functions supporting telecommunications services of collective interest, while expressly excluding infrastructure used solely for signal transduction or physical interconnection, such as base stations and PoPs (**Art. 3.2.1**). A Data Center that integrates Telecommunications Networks (DCTC) is defined as a facility that hosts and operates IT and telecommunications equipment with the security, resilience, and support systems necessary to sustain such services (**Art. 4.1.1**), and a DCTC Operator is any entity responsible for managing or providing that infrastructure, including both telecommunications providers and third-party infrastructure suppliers (**Art. 4.1.3**).

As written, this approach raises numerous concerns.

First, Articles 3 and 4 mischaracterize how cloud services operate by defining regulated infrastructure through broad functional criteria such as hosting, storage, and data processing (Articles 3.1.1–3.1.3), without distinguishing infrastructure that operates or controls public telecommunications networks from general-purpose digital infrastructure used as a third-party input. Cloud service providers do not provide regulated telecommunications services, do not perform core telecommunications functions such as operating public access networks, managing numbering resources, controlling radiofrequency spectrum through licensed assignments, performing call routing, signalling, or traffic management, and do not perform network control or switching functions; rather, they act as vendors of ancillary services to licensed telecommunications providers.

Second, Articles 3 and 4 fail to provide clear attribution of regulatory obligations and liability in environments characterized by layered commercial and technical arrangements. The Draft does not establish objective criteria for determining which entity would be deemed responsible

where telecommunications operators rely on cloud services; and where cloud providers, in turn, rely on colocation vendors for physical facilities, with no single entity exercising end-to-end control. The implicit assumption of a single "data center operator" responsible for compliance creates legal uncertainty regarding responsibility allocation and enforcement.

Third, the functional framing in Articles 3.1.1–3.1.3 presupposes levels of visibility into service criticality, customer workloads, and operational impacts that are incompatible with established cloud operating models. Under shared-responsibility architectures, cloud providers secure the underlying infrastructure, while telecommunications operators retain control over applications, configurations, and service delivery to end users. As a result, cloud providers generally cannot assess workload criticality or customer-specific service impacts, making the application of Articles 3 and 4 to such infrastructure technically infeasible.

Finally, Article 3 adopts an overbroad scope, particularly through Articles 3.1.2 and 3.1.3, which risk capturing virtually any infrastructure that processes telecommunications-related data, regardless of whether it performs core telecommunications network functions. Absent clear limiting criteria tied to network control or traffic management, this approach would inadvertently sweep general-purpose data centers, cloud services, and content delivery networks into scope solely because they support telecommunications workloads, rendering the Draft overinclusive from both legal and technical perspectives.

Given these concerns, CCIA recommends that ANATEL undertake the following revisions:

- Articles 3.1 and 3.1.1–3.1.3 should be revised to limit the scope of the regulation to infrastructure that is structurally and functionally integrated into the core operation of public telecommunications networks and that performs clearly defined core network functions, such as network control, signaling, switching, or traffic management. References to hosting, storage, and data processing should apply only where such activities are inseparable from network operation, and not to general-purpose or enterprise IT functions.
- To prevent overinclusive application, Articles 3.1.2 and 3.1.3, read together with the definition of DCTC in Article 4.1.1, should expressly exclude general-purpose digital infrastructure and industry-agnostic services, including compute, storage, hosting, databases, and content delivery networks, even where such infrastructure is used by telecommunications providers as enterprise customers.
- Article 4.1.1 should be narrowed so that a "Data Center that integrates Telecommunications Networks (DCTC)" refers only to data centers embedded in and operated as part of telecommunications networks under the control of licensed telecommunications providers of collective interest (common carriers), avoiding capture of standalone or shared digital infrastructure outside ANATEL's mandate.
- Article 4.1.3 should be amended to clarify that the "DCTC Operator" is the licensed telecommunications service provider bearing primary and non-delegable responsibility for service quality, continuity, and security, and that suppliers or administrators of physical or logical infrastructure are not subject to direct approval, inspection, or enforcement by ANATEL.
- Finally, Articles 3.1 and 4.1.1 should clarify that infrastructure is not brought into scope solely because it processes data related to Brazilian telecommunications services,

including where such infrastructure is located outside Brazil; applicability should turn on functional integration into the telecommunications network, not data location or incidental support of telecommunications workloads.

Current Text	Proposed Text
3.1. This document covers infrastructure that is part of telecommunications networks and performs the following functions:	*3.1. This document covers infrastructure that is ~~part~~* ***owned, operated, or directly controlled by telecommunications service providers of collective interest services, and that are structurally and functionally integrated into the core operation*** *of* ***public*** *telecommunications networks****, used for the execution of core functions essential for the continuity of the provision of telecommunications services of collective interest,*** *and performs the following functions:*
3.1.1. Hosting of computer systems that are part of the functional core of telecommunications services of collective interest, essential for their continuity;	*3.1.1. Hosting of computer systems that are part of the* ***network control, signaling, switching, or traffic-management*** *functional* ***and essential*** *core of telecommunications services of collective interest, essential for their continuity;*
3.1.2. Storage of data necessary for the operation and use of telecommunications services of collective interest; or	*3.1.2. Storage of data* ***strictly*** *necessary* ***for the execution of core telecommunications network functions****, for the operation ~~and use~~ of telecommunications services of collective interest; or*
3.1.3. Execution of network functions that support telecommunications services of collective interest and that process data from these services and their users.	*3.1.3. Execution of* ***core*** *network functions that* ***are indispensable to the operation of*** *~~support~~ telecommunications services of collective interest and that process data from these services and their users,* ***excluding general-purpose data processing or enterprise IT functions****.*
3.2. This document does not cover infrastructure intended exclusively for:	*3.2. This document does not* ***apply to:*** *~~cover infrastructure intended exclusively for~~*
3.2.1. Performing signal transduction, distribution, or physical interconnection functions, including, among others, points of presence (PoP), base stations, and their control equipment.	*3.2.1. Performing signal transduction, distribution, or physical interconnection functions, including, among others, points of presence (PoP), base stations, and their control equipment.*
	3.2.2. Infrastructure pertaining to cloud and other digital services offered

	commercially to customers across multiple industries, even in the case where such infrastructure is also used by telecommunications service providers as enterprise customers. ***3.2.3. Infrastructure pertaining to and provision of services to Value-Added Service providers for content acceleration or distribution, edge caching, or any service primarily designed to optimize content delivery to end users.*** ***3.2.4. Infrastructure intended exclusively for the performance of Business Support Systems (BSS) functions, including customer management, product management, order management, revenue management, and billing operations.*** ***3.2.5. Infrastructure intended exclusively for the performance of Operations Support Systems (OSS) functions, including network management, service provisioning, service assurance, network inventory management, and fault management operations.***
4.1. For the purposes of this document, in addition to the definitions contained in Anatel's regulations, the following definitions apply: *4.1.1. Data Center that integrates Telecommunications Networks (DCTC): structure, or group of structures, dedicated to the centralized accommodation, interconnection, and operation of information technology equipment and telecommunications networks, capable of providing data storage, processing, and transport services in conjunction with all power distribution and environmental control facilities and infrastructure, together with the necessary levels of recovery and security*	*4.1. For the purposes of this document, in addition to the definitions contained in Anatel's regulations, the following definitions apply:* *4.1.1. Data Center that integrates Telecommunications Networks (DCTC): structure, or group of structures, dedicated to the centralized accommodation, interconnection, and operation of information technology equipment* ~~*and*~~ ***structurally and functionally integrated into*** *telecommunications networks,* ***and used for the execution of functions essential to the continuity of the provision of telecommunications services of collective interest****, capable of providing data storage, processing, and transport services* ***that are inseparable from core telecommunications network operations***

	in conjunction with all power distribution and environmental control facilities and infrastructure, together with the necessary levels of recovery and security
4.1.3. DCTC Operator: the legal entity applying for approval, responsible for the management, operation, or provision of the physical or logical infrastructure necessary for the operation of a DCTC, including processing, storage, and hosting environments for applications or services used to support telecommunications services of collective interest, which may include: a) the telecommunications service provider that implements and operates its own data center; b) the supplier, provider, or administrator of physical or logical data center infrastructure, whose structure can be used by providers to support functions essential to the continuity and operation of telecommunications services.	*4.1.3. DCTC Operator: the ~~legal entity~~* ***licensed telecommunications service provider of collective interest (common carrier)*** *applying for approval, responsible for the management, operation, or provision of the physical or logical infrastructure necessary for the operation of a DCTC, including processing, storage, and hosting environments for applications or services used to support telecommunications services of collective interest, which may include: a) the telecommunications service provider* ***of collective services interest*** *that implements and operates its own* ***DCTC*** *~~data center~~; b) the supplier, provider, or administrator of physical or logical data center infrastructure,* ***whose business is wholly dedicated to serving, on a contractual basis to licensed telecommunications service providers of collective interest, without assuming the status of DCTC Operator or being subject to direct approval, inspection, or enforcement by ANATEL****, whose structure* ***is*** *~~can be~~ used by providers to support functions essential to the continuity and operation of telecommunications services.*

Technical Requirements

Section 5.2.1 allows DCTC conformity to be demonstrated through third-party certifications, but conditions direct approval by ANATEL on submission of a complete, cumulative set of certifications covering all technical, security, environmental, and energy-management requirements listed in the Annex.

As drafted, Section 5.2.1 effectively adopts an all-or-nothing certification model by requiring operators to present the full bundle of referenced standards (e.g., ISO/IEC 27001, ISO/IEC 22237 or TIA-942-C, ISO 14001, and ISO 50001), regardless of the operator's existing compliance profile. This approach is disproportionate and economically inefficient. It penalizes data center operators that already comply with industry best practices and hold widely recognized certifications covering substantial portions of the requirements, while compelling duplicative audits and certifications solely to satisfy formal completeness. In addition, the exclusive focus on ABNT-ISO certifications fails to recognize equivalent, internationally accepted standards (e.g., IEC, EN, ANSI, SOC) that meet or exceed the same technical

objectives, thereby creating costs without delivering commensurate security, resilience, or sustainability benefits.

ANATEL should adopt a more proportionate and modular framework that allows operators to rely on certifications they already hold, recognizes equivalent international certifications where technical requirements are identical or more stringent, and permits any uncovered requirements to be addressed through targeted assessments, whether via an OAS or equivalent verification, rather than mandating submission of a complete certification set in all cases.

Current Text	Proposed Text
5.2.1. The conformity of the DCTC may be proven by presenting certifications issued by other certification bodies, provided that they comply with the relevant reference standards and are equivalent to the technical requirements set forth in this Annex. *In such cases, in order for DCTC operators to apply for approval directly to Anatel, without the need for evaluation by an OAS, a complete set of certificates covering all the requirements established in this Annex must be presented, such as the following certificates:* *a) ABNT-ISO/IEC 27001, referring to the Information Security Management System (ISMS);* *b) ABNT-ISO/IEC 22327, or ANSI/TIA-942C, referring to physical infrastructure, continuity, and operational security requirements;* *c) ABNT-ISO/IEC 14001, referring to the Environmental Management System (EMS);* *d) ABNT-ISO/IEC 50001, referring to the Energy Management System (EMS).*	*5.2.1. The conformity of the DCTC may be proven by presenting certifications issued by other certification bodies, provided that they comply with the relevant reference standards and are equivalent to the technical requirements set forth in this Annex.* *In such cases, in order for DCTC operators to apply for approval directly to Anatel, without the need for evaluation by an OAS, ~~a complete set of~~ certificates covering all the* ***applicable*** *requirements established in this Annex must be presented, such as the following certificates**, or equivalent certifications demonstrating compliance with the same technical requirements**:* *a) ABNT-ISO/IEC 27001, referring to the Information Security Management System (ISMS)**, or equivalent**;* *b) ABNT-ISO/IEC 22327, or ANSI/TIA-942C, referring to physical infrastructure, continuity, and operational security requirements**, or equivalent**;* *c) ABNT-ISO/IEC 14001, referring to the Environmental Management System (EMS)**, or equivalent**;* *d) ABNT-ISO/IEC 50001, referring to the Energy Management System (EMS)**, or equivalent**.*

Sections 5.2.2 and **5.2.2.1** allow a single application to cover multiple DCTCs where the infrastructures are considered equivalent, defining equivalence as having the same function, topology, Availability Class, Protection Classes, and risk analysis requirements. This framework

is intended to streamline compliance for organizations operating multiple facilities with comparable architectures.

The Draft's definition of "equivalence" is overly rigid, however, as it requires identical functions, topology, and classification levels, without accommodating reasonable variations in facility size, equipment models, or site-specific adaptations that do not affect security, resilience, or service continuity. In practice, this narrow definition risks forcing operators to submit separate documentation for each facility, even where infrastructures are substantially similar, creating hefty administrative burdens.

ANATEL should permit the use of standardized documentation for substantially similar facilities, supplemented by concise annexes describing site-specific differences, rather than requiring strict identity across all equivalence criteria.

Current Text	Proposed Text
5.2.2. The application may cover sets of DCTCs in order to demonstrate the equivalence or interrelationship between infrastructures for compliance with requirements. *5.2.2.1. Infrastructure Equivalence is understood to mean when multiple sites of the organization have the same function, topology, Availability Class, and Protection Classes, as well as equivalence in the requirements adopted in the Risk Analysis Policy.*	*5.2.2. The application may cover sets of DCTCs in order to demonstrate the equivalence or interrelationship between infrastructures for compliance with requirements.* *5.2.2.1. Infrastructure Equivalence is understood to mean when multiple sites of the organization have ~~the same~~ **substantially similar** function **and** topology, **equivalent** Availability Class and Protection Classes, ~~as well as equivalence in the~~ **and consistent** requirements adopted in the Risk Analysis Policy, **allowing for site-specific variations that do not affect compliance with the applicable requirements**.*

Sections 5.3.1 and **5.4.2.1** require DCTC operators to compile and maintain highly detailed architectural, security, and risk documentation, including floor plans, system diagrams, and comprehensive risk assessments, the disclosure of which could expose sensitive operational and security information if not subject to strict confidentiality and access controls.

Mandatory submission of detailed floor plans, system diagrams, and risk analysis policies creates a material security risk, as improper disclosure could provide a roadmap for physical attacks, sabotage, or unauthorized access, directly undermining the Draft's stated objective of enhancing infrastructure security. Because compliance can already be verified through accredited certifications or OAS audits, there is no clear justification for ANATEL to collect or retain such highly sensitive materials; any necessary review should occur on-site or under secure audit conditions.

ANATEL should revise the Draft to avoid requiring submission or retention of detailed floor plans and risk analysis documentation, limiting review of such materials to on-site or secure

audit procedures conducted by accredited bodies or OASs. If submission is maintained, the Draft should expressly classify these materials as permanently confidential, restrict access to a narrow set of authorized personnel, and impose clear secure-handling and breach-notification obligations.

Current Text	Proposed Text
5.3.1. The DCTC operator shall prepare and maintain an updated Descriptive Memorandum that consolidates the essential information of the DCTC project, in accordance with the provisions of Clause 9.1 of ISO/IEC 22237-1 and the Risk Analysis Policy (item 5.4 of this document), which shall contain, at a minimum:	*5.3.1. The DCTC operator shall prepare and maintain an updated Descriptive Memorandum that consolidates the essential information of the DCTC project,* ***which shall be maintained by the DCTC operator and made available for review by an OAS or ANATEL under secure and confidential conditions****, in accordance with the provisions of Clause 9.1 of ISO/IEC 22237-1 and the Risk Analysis Policy (item 5.4 of this document), which shall contain, at a minimum:*
a) a description of the redundancy architecture of the power, air conditioning, and telecommunications systems, compatible with the declared Availability Class and with the criteria in Table B.1 of ISO/IEC 22237-1, as well as with the other parts of the ISO/IEC 22237 series applicable to each system, accompanied by floor plans, singleline diagrams, capacity calculations, and other relevant details of the installation;	*a) a description of the redundancy architecture of the power, air conditioning, and telecommunications systems, compatible with the declared Availability Class and with the criteria in Table B.1 of ISO/IEC 22237-1, as well as with the other parts of the ISO/IEC 22237 series applicable to each system, accompanied by floor plans, singleline diagrams, capacity calculations, and other relevant details of the installation,* ***which may be reviewed on-site or under secure audit conditions and shall be treated as confidential information****;*
b) a description of the Physical Protection Classes assigned to the areas of the facility, protection against unauthorized access, internal environmental events, and external environmental events, correlated with the risks identified in the Risk Analysis Policy, including floor plans indicating the classified areas, their physical boundaries, and other relevant details of the implementation;	*b) a description of the Physical Protection Classes assigned to the areas of the facility, protection against unauthorized access, internal environmental events, and external environmental events, correlated with the risks identified in the Risk Analysis Policy, including floor plans indicating the classified areas, their physical boundaries, and other relevant details of the implementation****, subject to confidentiality and secure-handling requirements****;*
5.4.2.1. As a general technical requirement, the Risk Analysis Policy must include, at a minimum:	*5.4.2.1. As a general technical requirement, the Risk Analysis Policy****, which shall be subject to appropriate confidentiality and secure-handling requirements,*** *must include, at a minimum:*

a) Definition of the scope and coverage of the Risk Analysis Policy in physical, organizational, and technological dimensions, detailing: physical units, infrastructure, assets, sectors, and processes to which the policy applies.	*a) Definition of the scope and coverage of the Risk Analysis Policy in physical, organizational, and technological dimensions, detailing: physical units, infrastructure, assets, sectors, and processes to which the policy applies.*
b) Identification of risks, listing events that could cause service interruption or degradation, including: power failures, mechanical failures, fire, unauthorized physical access, internal and external environmental events, human error, cybersecurity incidents, and telecommunications incidents.	*b) Identification of risks, listing events that could cause service interruption or degradation, including: power failures, mechanical failures, fire, unauthorized physical access, internal and external environmental events, human error, cybersecurity incidents, and telecommunications incidents.*
c) Impact assessment, describing the operational, financial, and continuity consequences of each identified risk.	*c) Impact assessment, describing the operational, financial, and continuity consequences of each identified risk.*
d) Probability assessment, considering failure history, environmental conditions, facility characteristics, known vulnerabilities, and maturity of operational processes.	*d) Probability assessment, considering failure history, environmental conditions, facility characteristics, known vulnerabilities, and maturity of operational processes.*
e) Recovery time estimation, predicting rapid, moderate, or prolonged recovery scenarios, depending on the nature of the incidents assessed.	*e) Recovery time estimation, predicting rapid, moderate, or prolonged recovery scenarios, depending on the nature of the incidents assessed.*
f) Planned or existing mitigation measures, including technical, operational, and organizational controls designed to reduce the probability or impact of identified risks.	*f) Planned or existing mitigation measures, including technical, operational, and organizational controls designed to reduce the probability or impact of identified risks.*

Conclusion

This Public Consultation presents an important opportunity to strengthen the resilience of Brazil's telecommunications networks while ensuring that regulatory obligations remain clear, proportionate, and firmly grounded in the LGT. By refining the scope and definitions to focus on operators of licensed telecommunications services of collective interest (common carriers) and clearly defined core telecommunications functions, and by avoiding duplicative requirements on general-purpose digital infrastructure, ANATEL can enhance legal certainty and support continued investment in Brazil's digital ecosystem. CCIA appreciates the opportunity to provide these comments and looks forward to continued engagement.