WRNP MAGAZINE

27 Workshop RNP

May
2026

WRNP 2026 highlights

quantum technologies, artificial intelligence, and cybersecurity

Interviews

RNP Director-General Lisandro Granville
discusses digital sovereignty

MCTI and the Brazilian AI Plan
Research networks, supercomputing, and specialist training: Brazil in the global AI race

And more:

Explore our initiatives and platforms for experimentation, network monitoring, blockchain, open networking, and innovation

RNP

May

25-27

BAHIA

Access the materials shared during the 27th WRNP at:

RNP *TECH NEWS*

Exploring the future of open and intelligent networks — and many other topics that matter to you!

RNP Tech News is RNP's technical-scientific newsletter, distributed through the professional social network LinkedIn. Published every two months, it features articles of interest written by network researchers and other professionals working in the field of innovation. In addition, the newsletter follows major trends in Information and Communication Technologies (ICTs), both in Brazil and internationally.

Subscribe and follow us here.

RNP

MINISTÉRIO DA **CULTURA**

MINISTÉRIO DA **DEFESA**

MINISTÉRIO DA **SAÚDE**

MINISTÉRIO DAS **COMUNICAÇÕES**

MINISTÉRIO DA **EDUCAÇÃO**

MINISTÉRIO DA **CIÊNCIA, TECNOLOGIA E INOVAÇÃO**

BRAZILIAN GOVERNMENT

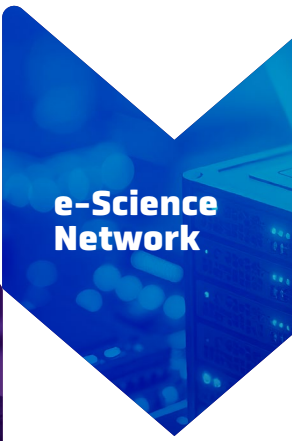
BRASIL

STANDING WITH THE BRAZILIAN PEOPLE

WRNP MAGAZINE

27 Workshop RNP

May
2026



MASTHEAD

WRNP Magazine – 27th WRNP

Brazilian National Research and Education Network (RNP)

Director-General: Lisandro Zambenedetti Granville

27th WRNP Organizing Committee:

General Coordination: Iara Machado

Executive Coordination: Leandro Ciuffo and Luciana Ferreira

Program Committee Coordination: José Ferreira de Rezende and Davi Gemmer

Communication and Marketing Management: Stela Tsirakis

Communication and Marketing Coordination: Fábio Falcão Cazes and Rafael Haruo Horigome

Startup Arena, Exhibitions, and Demonstrations: Rafael Valle and Ana Georgia Barbosa

Editorial, Graphic Design, and Creative Project: Corcovado Comunicação Estratégica

Graphic Design Project: Andréa Miranda

Layout: F/damatta Design

Content Production and Review: Larriza Thurler, Ana Carolina Landi, Jaime Sousa Jr.

Photography: Shutterstock and the RNP image archive

RNP

MINISTÉRIO DA CULTURA | MINISTÉRIO DA DEFESA | MINISTÉRIO DA SAÚDE | MINISTÉRIO DAS COMUNICAÇÕES | MINISTÉRIO DA EDUCAÇÃO | MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO

BRAZILIAN GOVERNMENT BRASIL STANDING WITH THE BRAZILIAN PEOPLE

Welcome to the **27th WRNP** in Praia do Forte, Bahia

It is with great satisfaction that we welcome participants to WRNP 2026, held this year in the inspiring setting of Praia do Forte, Bahia. By bringing together researchers, managers, specialists, entrepreneurs, and partners from the innovation ecosystem, this event reaffirms the commitment of the research and education community to advancing technology and building a more collaborative and sustainable digital future.

For more than two decades, Workshop RNP has served as a space for converging ideas, experiences, and projects that drive the development of information and communication technologies applied to education and science. Throughout these days, participants will have the opportunity to explore innovative initiatives, follow research and development projects, take part in technical panels and discussions on themes shaping the future of advanced networks and their services.

Photo: RNP

This year's program has been carefully designed to promote the exchange of knowledge and strengthen connections among academia, government, companies, and startups. Topics such as artificial intelligence applied to academic networks, international cooperation, quantum communication, and the role of universities in the development of national technologies are among the highlights participants will find in our discussions.

More than a technical event, WRNP is a collaborative environment. Here, ideas find partners, projects gain visibility, and new opportunities for cooperation emerge. It is also a space to strengthen our community and expand the impact of research and development initiatives for the benefit of education, research, and society.
We hope every participant makes the most of this opportunity for learning, networking, and inspiration. May the conversations initiated here turn into new partnerships, projects, solutions capable of driving innovation in Brazil and beyond.

Welcome to WRNP 2026.

IARA MACHADO
DIRECTOR OF RESEARCH, DEVELOPMENT, AND INNOVATION AT RNP

27th WRNP: looking toward the future

Photo: RNP

DEAR READERS,

In 2026, we introduce structural and symbolic changes that reflect the continuous evolution of the event.

For the first time, the WRNP was organized across **two venues.** On May 25 and 26, activities were held at the Praia do Forte Convention Center. On the morning of May 27, we were welcomed by the **Angelina Rodrigues Municipal School,** marking an unprecedented gesture of engagement with the local community and reinforcing RNP's commitment to the democratization of science and technology. As a counterpart for the use of the school facilities, the WRNP organization deployed improvements in the classrooms used during the event, leaving a legacy for the school.

Traditionally, the WRNP has always taken place during the first two days of the SBRC. This year, we also innovated by extending our activities into a **third day,** featuring a session dedicated to updates on regional research infrastructure projects, as well as the first meeting of the **Network of Startups supported by RNP.**

We are also delighted to momentarily bring back our colleague Daniela Brauner, former RNP R&D manager and an active contributor to previous editions of the WRNP. Now working at Géant—the European association of academic networks—Daniela brings an international perspective on Artificial Intelligence, significantly enriching our program.

Another major milestone is the implementation of a structured action to promote **gender diversity**. For the first time, we granted registration-fee waivers to female students, encouraging the participation of young women in ICT and strengthening representation at the event.

Finally, we celebrate an important editorial achievement: we produced the **fifth edition of this magazine,** distributed to WRNP participants, and for the first time also released a **digital English version,** expanding the international reach of RNP's R&D initiatives and reinforcing our global presence.

May WRNP 2026 be inspiring, inclusive, and filled with transformative connections! •

LEANDRO CIUFFO
EXECUTIVE COORDINATOR
OF THE 27TH WRNP

27 Workshop RNP

LISANDRO GRANVILLE

Photo: RNP

Lisandro Granville, RNP Director-General

'Digital sovereignty is not isolation, it is the autonomy to choose',

says **Lisandro Granville**

ACCORDING TO RNP'S DIRECTOR-GENERAL, BRAZIL MUST BE PREPARED FOR CRITICAL SCENARIOS

BY **HENRIQUE GIMENES**

Discussions around digital sovereignty have gained momentum in recent years, driven mainly by the growing dependence on data, platforms, and technological infrastructures. The topic has become part of the development agendas of countries seeking to strengthen their scientific and innovation capabilities, including Brazil.

In the fields of science and education, digital sovereignty plays an even more strategic role, since it is necessary to ensure advanced connectivity, security, digital identity, and processing capacity. For RNP's Director-General, Lisandro Granville, achieving sovereignty does not mean isolating the country from the international landscape. On the contrary, cooperation is what enables countries to expand capabilities, share knowledge, and build safer and more sustainable technological alternatives.

In this interview with the **WRNP MAGAZINE,** Granville analyzes the challenges of digital sovereignty in Brazil and discusses how academic networks and shared infrastructures can help reduce technological dependencies and strengthen the country's innovation capacity.

WRNP MAGAZINE: **Digital sovereignty is a topic that has frequently appeared in the media. In practical terms, what does digital sovereignty mean for Brazil today?**

LISANDRO GRANVILLE: It is the ability of a country to make informed, sustainable, and executable choices regarding critical infrastructures, data, and technologies — and to sustain those choices through governance, security, technical expertise, and predictable investments. This includes everything from connectivity, identity, and cybersecurity to storage, processing, digital platforms, and data management. It is not about "producing everything locally" or denying global interdependence; it is about reducing dependencies that, in critical moments, can become operational bottlenecks, unpredictable costs, or limitations on decision-making.

In Brazil's case, digital sovereignty is especially relevant because both the economy and the public sector are moving toward increasingly deep digitalization, while data and computing capacity become strategic assets. Having sovereignty therefore means being able to establish requirements (such as continuity, auditability, data protection, interoperability, portability, and compliance) and having real alternatives whenever a technology, provider, or contractual arrangement no longer serves the public interest. In other words: sovereignty is not isolation; it is the autonomy to choose responsibly.

In the context of academic networks and the science, technology, and innovation system, this means ensuring that the infrastructure supporting education, research, and innovation (advanced connectivity, identity federation, digital services, data, and security) is aligned with national objectives and with trust arrangements compatible with the public mission of institutions.

WRNP MAGAZINE: **Why has this topic become so strategic in recent years, especially given the acceleration of digital transformation and artificial intelligence?**

LISANDRO GRANVILLE: Digital transformation had already been advancing, but artificial intelligence accelerated the process and raised the level of demands: more data, more computing, more connectivity, and more security. AI models depend on massive volumes of data, intensive processing environments, and complex chains of software, services, and infrastructure. When these components are concentrated in the hands of a few players, this affects not only pricing, but also timelines, availability, technical requirements, interoperability standards, and even terms of use. For a country, this becomes a strategic issue because it affects economic

competitiveness, scientific capacity, and the continuity of critical services. In addition, the international landscape has made it increasingly clear that technological dependencies can quickly turn into vulnerabilities due to trade restrictions, unilateral platform policy changes, product discontinuation, abrupt cost increases, or contractual requirements that may conflict with the public interest. As a result, the debate is no longer merely technical: it now involves development strategy, skills training, long-term sustainability, and coordination capacity among government, academia, and private sector.

WRNP MAGAZINE: **What are the main risks for a country that relies excessively on foreign technologies? And how can we avoid treating this debate in an oversimplified way, as if sovereignty meant isolation?**

LISANDRO GRANVILLE: The risks manifest themselves in three main dimensions. The first is technical and operational: service continuity, incident response capacity, auditing, transparency, and control over critical components. The second is economic: dependency can lead to rising costs, limited budget predictability, and technological lock-in, when migration becomes too expensive or even unfeasible. The third is strategic: critical dependencies reduce a country's decision-making margin in times of crisis, geopolitical tensions, or regulatory and commercial changes. To avoid oversimplifications, it is important to make one thing very clear: digital sovereignty is not about closing doors. Science is collaborative and international by nature; academic networks exist precisely to enable that collaboration. The key point is to build alternatives, portability, and negotiation capacity, reducing dependencies on structural components. Rather than framing the discussion simply as "national versus foreign," we should ask which assets are critical, which requirements are non-negotiable (such as security, compliance, continuity, and interoperability), which parts can safely be outsourced, and which require trust and governance arrangements more closely aligned with the public interest.

WRNP MAGAZINE: **Does digital sovereignty mean pursuing total self-sufficiency, or is it possible to think about hybrid models with diversified partnerships and suppliers?**

LISANDRO GRANVILLE: Total self-sufficiency is ultimately utopian and, in many cases, undesirable. A more consistent path is to adopt hybrid models that combine supplier and technological diversification; strengthening local capabilities; investing in research and innovation; and establishing governance and contractual arrangements that avoid irreversible dependencies. Diversification reduces systemic risk: when one solution fails, becomes more expensive, or changes its rules, the system is not trapped in a single path. Strengthening local expertise is also essential so that the country can evaluate, operate, integrate, audit, and evolve technologies, even when part of them is acquired externally. In this sense, sovereignty is less about "manufacturing everything" and more about having the architectural, engineering, and governance

Photo: Elea

Generators at RNP's National Data Center at Elea, in São Paulo

capacity: decide, integrate, and sustain technological choices aligned with long-term national interests.

WRNP MAGAZINE: **How can universities and public institutions balance the search for technological autonomy with the need for economic efficiency?**

LISANDRO GRANVILLE: Public institutions and universities need efficiency and sustainability. Developing everything locally is not always the best short-term solution and, in many cases, it is not even the role of each institution individually. The balance requires looking at total cost and risk: not only the initial price, but also maintenance, evolution capacity, dependencies, compliance, security, and continuity. Solutions that appear "cheap" at first may become costly when institutions become locked into a technology, budgets fluctuate, or security requirements increase. This is where shared infrastructures and cooperative arrangements become important: when the system is organized, it gains scale, standardizes what should be standardized, and distributes costs rationally. A national infrastructure such as RNP exists precisely to reduce duplication, raise security levels, and allow universities and research centers to avoid "reinventing" complex components independently. In this model, autonomy does not mean that each institution must build everything on its own; it means the system collectively has the capacity to sustain strategic services with quality and governance.

WRNP MAGAZINE: **Why is digital sovereignty especially relevant for education, science, and innovation environments?**

LISANDRO GRANVILLE: Because education and science deal with knowledge production, sensitive data, and strategic research, including personal data, intellectual property, research results, and projects with high scientific and technological value. If the digital infrastructure supporting these activities is fragile, insecure, or excessively dependent, the impact directly affects innovation capacity: from data leaks and service interruptions to restrictions on data usage and limitations on large-scale collaboration. Furthermore, universities are where we train the professionals who will design, operate, and protect the country's digital infrastructures. Therefore, digital sovereignty involves skills development and workforce training, but also providing real environments for experimentation and technological evolution. Academic infrastructure is not merely a "support tool"; it is part of the innovation ecosystem itself.

WRNP MAGAZINE: **How does RNP contribute structurally to strengthening digital sovereignty in Brazil?**

LISANDRO GRANVILLE: RNP contributes structurally by combining three dimensions: national infrastructure, trust mechanisms, and advanced shared services. By operating a high-capacity national academic network connecting institutions across the country,

"THE ECONOMY AND THE PUBLIC SECTOR ARE MOVING TOWARD AN INCREASINGLY DEEP DIGITALIZATION."

RNP sustains a strategic asset for education, research, and innovation. But its contribution goes beyond connectivity: RNP enables trust arrangements for the ecosystem (such as identity and federations) in addition to services and platforms that reduce costs, increase maturity, and reinforce the system's autonomy. There is also an essential component: RNP acts as an integration and experimentation environment for the academic community and for strategic projects, helping transform the system's needs into scalable, evolutionary solutions with governance. This reduces critical dependencies not through imposed measures, but through the development of standards, cooperation, engineering capacity, security, and continuity.

WRNP MAGAZINE: **In practical terms, how does RNP support universities and research centers in this process?**

LISANDRO GRANVILLE: In practice, RNP provides high-capacity connectivity and operates the National Data Centers (CNDs), which support advanced services and infrastructure environments for shared demands. In cybersecurity, RNP maintains a Security Operations Center (SOC) and initiatives that help institutions improve their maturity levels, in addition to network coordination and incident response actions. This is complemented by digital identity solutions, collaboration services, and support for large-scale projects, all essential for enabling collaborative research, secure operations, and interoperability among institutions. This entire structure is only possible because RNP has nationwide reach through its Points of Presence (PoPs). That reach depends on cooperative arrangements with host institutions — typically universities and research institutes — which enable local operations, campus integration, and relationships with user communities. There is also a critical distributed human resources component, with teams operating and maintaining the PoPs across all 27 Brazilian states, ensuring continuity, incident response, technical evolution, and compliance with security and governance requirements.

The result is twofold: universities and research centers can focus on their missions without needing to build the entire technological foundation from scratch, while also advancing governance, processes, and capacity-building with greater predictability and autonomy. In terms of digital sovereignty, this arrangement is particularly relevant because it creates a trusted infrastructure at scale that would be very difficult to achieve through fragmented initiatives.

WRNP MAGAZINE: **How does RNP engage with international academic networks, and what lessons does this exchange bring to Brazil's technological autonomy?**

LISANDRO GRANVILLE: Interaction with international academic networks is essential to keep Brazilian research connected to major global projects. But this dialogue goes far beyond high-capacity links: it involves continuous exchanges on governance, security, service architecture, operational models, and sustainability. By following what other national research and education networks are doing, we can compare strategies, learn from incidents and difficult decisions, and adopt stronger and more sustainable practices.

At the same time, sharing Brazilian initiatives strengthens our international presence and helps calibrate domestic priorities: the country expands its decision-making capacity when it deeply understands trade-offs and alternatives. For digital sovereignty, this is fundamental: autonomy is not built in isolation; it is built through knowledge, standards, cooperation, and the capacity to choose.

Photo: RNP

Granville: the importance of infrastructure, people, and institutional coordination for digital sovereignty

WRNP MAGAZINE: In your view, what are the main challenges for the next five to ten years? And what message would you leave to readers regarding RNP's role in this scenario?

LISANDRO GRANVILLE: Over the next five to ten years, I see three central challenges. The first is infrastructure: we need continuous and predictable investment in connectivity, security, data, and computing environments, keeping pace with the growing demand for AI and data-driven science. The second is people: training and retaining talent in engineering, data science, AI, and cybersecurity, with learning pathways and real operational environments. The third is institutional coordination: digital sovereignty requires long-term alignment among government, academia, and private sector, with consistent policies, clear governance, and sustainability.

The message I would leave is that digital sovereignty is not a project with a beginning, middle, and end. It is an ongoing agenda built through well-founded technical decisions and institutional cooperation. RNP will continue acting as a public infrastructure that articulates the education and research system, connecting institutions, providing trust mechanisms, improving security maturity, and sustaining shared services. In a world increasingly dependent on data and AI, this foundation is what enables the country to innovate with greater autonomy, responsibility, and capacity to choose. •

"AUTONOMY [...] MEANS HAVING THE COLLECTIVE CAPACITY TO SUSTAIN STRATEGIC SERVICES WITH QUALITY AND GOVERNANCE."

Photo: RNP

Henrique Miguel: "Academic networks and the national research infrastructure play a structural role within the PBIA"

Brazil in the global AI race

WITH INVESTMENTS OF R$ 23 BILLION THROUGH 2028, THE BRAZILIAN ARTIFICIAL INTELLIGENCE PLAN WILL EXPAND RESEARCH NETWORKS, SUPERCOMPUTING INFRASTRUCTURE, AND SPECIALIST TRAINING

BY **HENRIQUE GIMENES**

How can technological autonomy be ensured at a time when advances in Artificial Intelligence (AI) are becoming increasingly concentrated in the hands of a few companies and countries? The search for proprietary data infrastructure and computational capacity has become one of the main strategies for strengthening digital sovereignty. In Brazil, this effort has been structured through the Brazilian Artificial Intelligence Plan (PBIA), which brings together initiatives aimed at advancing AI development in the country.

With projected investments of R$ 23 billion through 2028, the PBIA was structured around five strategic pillars, with initiatives focused on advancing technological development in Brazil. These include strengthening computational infrastructure, training professionals, applying AI in public services, and fostering business innovation. According to Brazil's Ministry of Science, Technology and Innovation (MCTI), a significant portion of these initiatives has already entered the implementation phase.

"Based on monitoring completed in November 2025, the plan had already recorded financial execution of R$ 6.47 billion — equivalent to 28% of the total projected investment. Of the 54 structural actions, 30 had already delivered concrete results, while the others were still in their initial or preparatory stages," says Henrique Miguel, Secretary for Science and Technology for Digital Transformation at the MCTI.

One of the plan's main advances lies in the expansion of Brazil's high-performance computing infrastructure. The Santos Dumont supercomputer, operated by the National Laboratory for Scientific Computing (LNCC), was upgraded from 4.6 to 18.85 petaflops of processing capacity. The system now features a new architecture and graphics processing units (GPUs) designed for AI applications, expanding the scientific community's access to advanced computing resources.

"There is currently a critical dependence on foreign technologies, and this is not a problem exclusive to Brazil. Strengthening the national high-performance computing and AI infrastructure must be treated as a consistent long-term policy. Keeping pace with the speed of investments and innovations associated with artificial intelligence is also a challenge, and that is why it is essential to strengthen the national science, technology, and innovation ecosystem," Miguel points out.

The expansion of this technological capacity is also linked to the debate on digital sovereignty, which seeks to provide the country with the conditions to develop and operate strategic technologies such as data infrastructure, high-performance computing, and AI systems.

In this context, academic networks and the national research infrastructure play a central role by connecting educational and research institutions distributed throughout the country. This connectivity allows researchers from different regions to access advanced computational resources and collaborate on scientific projects that require large-scale data processing and exchange.

"Academic networks and the national research infrastructure play a structural role within the PBIA, as they support both the research, development, and innovation agenda and the training of talent essential to advancing AI in Brazil. The Brazilian National Research and Education Network (RNP) is the backbone of research, science, and education connectivity in the country," the secretary emphasizes.

TOWARD A BRAZILIAN AI ECOSYSTEM

A robust national infrastructure could also pave the way for the development of AI systems adapted to the Brazilian context, trained on the country's own data and content. This would expand the country's ability to create tools capable of better understanding the Portuguese language and the specificities of Brazilian society, reducing dependence on platforms developed abroad. Another important front involves organizing national datasets for AI training and supporting projects led by companies and educational and research institutions in the development of these technologies.

"To make this type of initiative viable, it is necessary to support science and technology institutions and companies operating in this field, creating the conditions needed to sustain qualified teams and continuous investments in research and development."

Photo: RNP

"Another challenge is keeping pace with the speed of investments and technological innovations associated with AI. It is necessary to support the entire national science, technology, and innovation ecosystem, prioritizing technological pathways that can generate greater returns for the country," Miguel highlights.

Training professionals capable of developing and applying artificial intelligence is one of the PBIA's central pillars. Expanding this talent base is seen as an essential condition for Brazil to keep pace with the rapid evolution of innovation in the sector. "This is the pillar with the highest percentage of actions already delivering results," Miguel explains. "In basic education, the 1st National AI Olympiad mobilized 716,000 students, and four Brazilian representatives participated in the international competition in Beijing in August 2025. In higher education, 8,104 new undergraduate positions in AI programs were created in 2024, surpassing the annual target of 5,000. Between 2022 and 2025, CNPq supported 773 master's students and 500 doctoral candidates in the field. Through 2028, R$ 194.2 million in undergraduate and graduate scholarships and R$ 152 million for doctoral studies abroad are planned," the secretary details. •

Secure communication in the quantum era

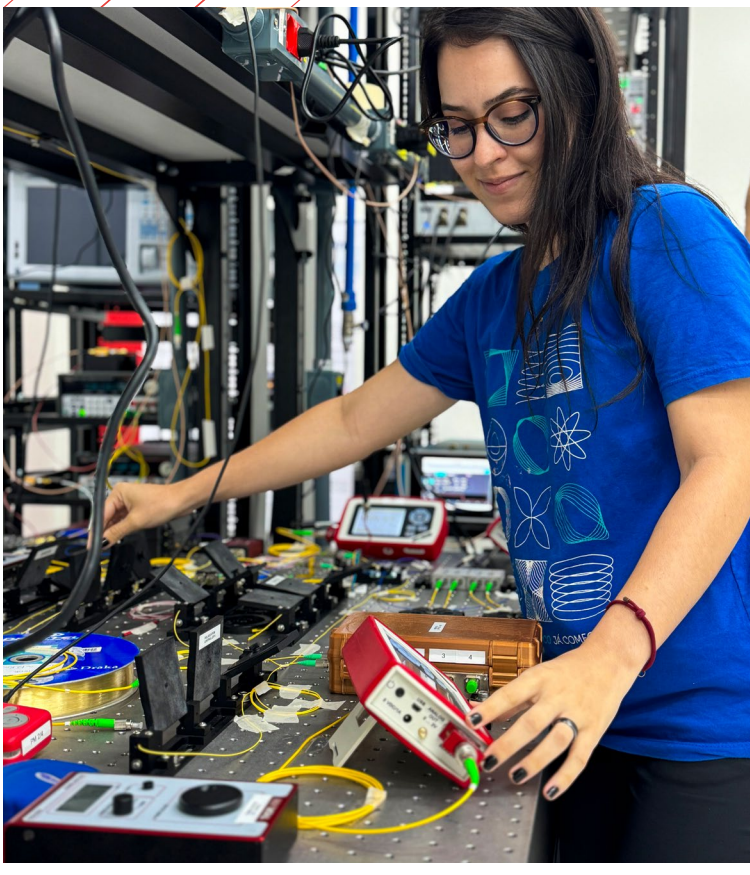
ADVANCES IN COMPUTING ARE DRIVING THE DEVELOPMENT OF NEW WAYS TO PROTECT DATA

BY **HENRIQUE GIMENES**

In an increasingly digitalized world, keeping data protected is no longer merely a technical concern; it has become a strategic issue. From the internet to academic and government networks, cryptography is one of the pillars supporting digital communication and online transactions. However, the next generation of processing — especially quantum computing — may redefine the security standards that currently structure data protection.

To address this potential scenario, researchers are working on what is known as quantum communication, a set of techniques that uses principles of quantum physics to make information exchange more secure. One of the best-known applications is quantum cryptography, mainly used in the generation and distribution of cryptographic keys. Unlike traditional systems, which are based on mathematical algorithms, this model was designed for a scenario in which computational power grows rapidly. In this context, protecting sensitive data, such as banking transactions and government communications, becomes increasingly important, as does ensuring greater digital sovereignty.

Photo: RNP



"In quantum cryptography, security is grounded in the laws of physics. No matter how much computing power you have, it is impossible to break the key without altering the system and being detected. Today, quantum computers are still unable to break the most robust keys, but progress is happening rapidly. That is why this transition must be carefully planned. It is not simply a matter of buying equipment and plugging it in as though everything was solved. It is a demanding process that requires organization and strategy," explains Valéria Loureiro, coordinator of the Embrapii (Brazilian Company for Industrial Research and Innovation) Competence Center for Quantum Technologies at Senai Cimatec, a Brazilian technology and innovation center.

The challenge lies not only in the technology itself, but also in preparing for its adoption. One of the first steps is understanding which security mechanisms are already in use and where the vulnerabilities lie. Many organizations still operate with outdated solutions, without a clear understanding of the level of protection they provide. In addition, it is necessary to ensure that communication infrastructure is prepared for this challenge. Brazil already has a large optical fiber infrastructure connecting the country, including academic networks and information highway projects in different regions, such as those operated by RNP. Even so, expanding and modernizing these networks may become necessary in order to keep pace with emerging technologies.

Photo: RNP

For Valéria, Brazil needs to prepare for a new era of digital security

"One of the major challenges is workforce development. There are still very few trained professionals in this field. Those who master the quantum side usually come from Physics and do not know how to do Engineering, while engineers are unfamiliar with Physics. Bringing these two worlds together is essential to bringing this technology to the market. If we fail to do so, we risk becoming dependent on fully imported technology and being forced to make this transition in a rush," Valéria points out.

WILL THE FUTURE OF COMMUNICATION BE QUANTUM?

Quantum communication is seen as an evolution of today's digital security technologies, but it is not expected to replace the traditional model of data transmission. The trend is for data to continue flowing through conventional communication systems, while cryptographic keys begin to be generated through quantum methods. In practice, this combination could enhance network security without requiring the replacement of the infrastructure already in operation.

Although still an emerging technology, quantum communication is already being used in some countries. Governments, universities, and

telecommunications companies have been testing different network models and evaluating how these solutions can be integrated into existing communication infrastructures.

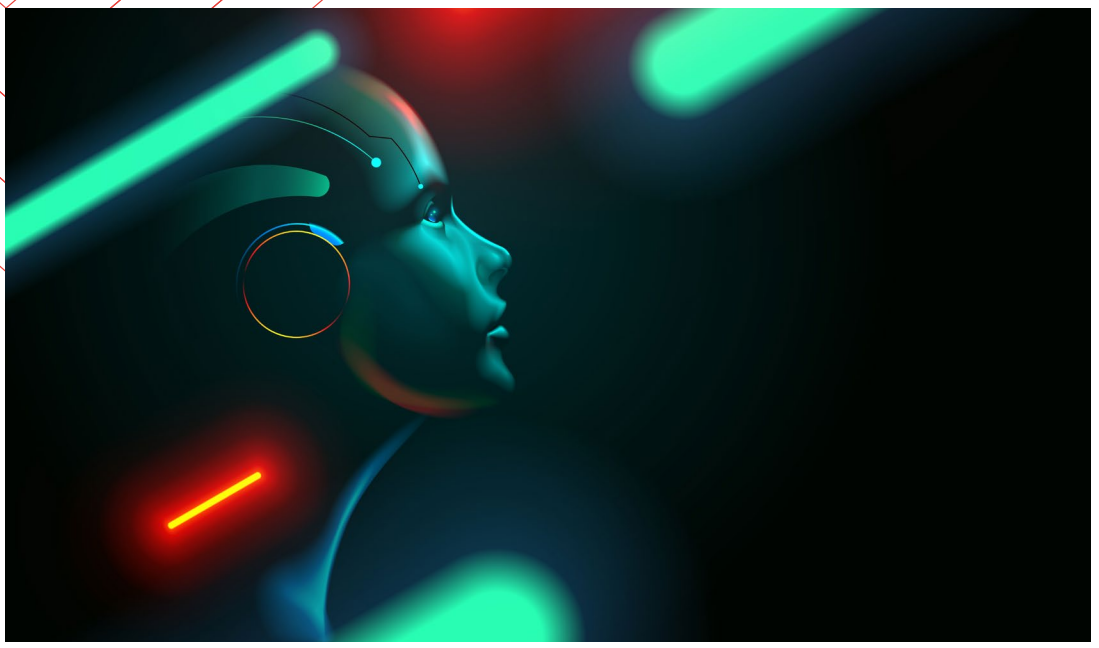
"China is among the countries most advanced in this field and already has operational networks, including in the banking sector. The Chinese have built a long-distance network connecting several cities and, within them, metropolitan networks that generate these cryptographic keys to protect communications. In Europe, several initiatives are also underway to test how this technology can function in practice," says the coordinator of the Embrapii Competence Center for Quantum Technologies at Senai Cimatec.

Another point under discussion concerns how these technologies should reach users. One possibility is the creation of private quantum networks by organizations that already operate their own optical fiber infrastructure, such as banks or government institutions. Another alternative would be offering quantum key generation as an additional security service provided by telecommunications operators.

Researchers are also working on solutions to address digital security in the era of quantum communication. One area gaining attention is so-called post-quantum cryptography. Unlike quantum communication, which generates cryptographic keys using principles of physics, this approach seeks to create new algorithms capable of resisting attacks from future quantum computers.

"Many people believe that post-quantum systems would be the evolution of quantum communication, but that is not exactly the case. They still rely on classical algorithms, only implemented in a much more complex way than what is currently used, with the expectation that a quantum computer will not be able to break them. But it is important to consider that, when we talk about quantum internet, this is still relatively far away. It could take 10 to 15 years. The trend is for quantum communication to be used only in applications that truly require a much higher level of security, while most traffic will continue to rely on traditional communication systems," emphasizes Valéria Loureiro. •

"MANY ORGANIZATIONS STILL OPERATE WITH OUTDATED SOLUTIONS, WITHOUT CLEARLY UNDERSTANDING THE LEVEL OF PROTECTION THEY PROVIDE."



The new generation of academic networks

BY **LARRIZA THURLER** AND **ANA CAROLINA LANDI**

For decades, academic networks were associated primarily with connectivity. Ensuring stable links among universities, research centers, and scientific institutions was the central mission of these infrastructures. Today, however, this role is rapidly expanding alongside the transformation of science itself.

One of the people who has closely followed this evolution is Daniela Brauner. A professor at Federal University of Rio Grande do Sul (UFRGS) and coordinator of the AI area at the European academic network GÉANT in Cambridge (United Kingdom), she has been connected to RNP since the beginning of her career, first working within the institution and later as a researcher collaborating on projects related to the Brazilian academic network.

"I have known RNP since the time when it was essentially a network infrastructure," she recalls. "At that time, while working in network support at a university, RNP mainly appeared in conversations whenever there were connectivity problems".

WITH THE ADVANCE OF AI, NRENS ARE EVOLVING FROM CONNECTIVITY INFRASTRUCTURES INTO DIGITAL PLATFORMS THAT INTEGRATE DATA, ADVANCED COMPUTING, AND NEW DIGITAL SERVICES FOR SCIENCE

Since then, however, the role of national research and education networks, the so-called NRENs, has expanded significantly. "NRENs are no longer just connectivity providers; they are becoming integrated digital platforms for science and education," she says. "They now have the opportunity to position themselves as strategic actors in the digital transformation of education and research ecosystems in their countries, while also playing an active role in national AI ecosystems".

THE IMPACT OF ARTIFICIAL INTELLIGENCE

The rise of artificial intelligence is accelerating this transformation. AI models require massive volumes of data, intensive computing infrastructure, and high-performance networks capable of connecting supercomputing centers, scientific repositories, and distributed research institutions.

In Europe, this movement has been accompanied by a coordinated strategy combining regulation, infrastructure investment, and the strengthening of the innovation ecosystem. Recent milestones include the EU AI Act, which establishes guidelines for the development of the technology, and initiatives such as the EuroHPC Joint Undertaking, focused on financing supercomputers and advanced infrastructure for AI.

Academic networks already occupied a central position, but in this scenario their role is also evolving. "Now, many of these organizations that already operated cloud or HPC services are evolving toward GPUs, data platforms, and even offering other services such as generative AI for teaching and research," Daniela explains. "NRENs are participating in major consortia with other organizations, collaborating on large-scale AI infrastructure projects across Europe".

THE CHALLENGE OF DIGITAL SOVEREIGNTY

The expansion of these capabilities is also connected to the debate on digital sovereignty and the attraction and retention of talent. "NRENs already operate sovereign connectivity infrastructures for universities and research institutes. Expanding this concept to other digital services seems like a natural path," Daniela observes.

In practice, many NRENs are acting as service integrators, offering Digital Research Environments and platforms that allow students and researchers to use generative AI tools while choosing among different models, often based on open technologies.

Another important element is the European coordination in negotiations with major cloud providers, through common contractual frameworks that strengthen the bargaining

"NRENS ALREADY OPERATE SOVEREIGN CONNECTIVITY INFRASTRUCTURES FOR UNIVERSITIES AND RESEARCH INSTITUTES."

power of academic institutions. At the same time, public policies have encouraged the development of open AI models and the strengthening of the European innovation ecosystem, including start-ups and small companies developing strategic technologies for science and education.

INTERNATIONAL COOPERATION AND DATA DIVERSITY

International cooperation therefore becomes even more relevant. According to Daniela, collaboration between Brazil and Europe can contribute to the development of more robust and representative AI models. "The cultural and scientific diversity between Europe and Latin America is extremely valuable for developing AI models with fewer biases," she says.

The sharing of scientific data also emerges as an important opportunity. Information from areas such as biodiversity, climate, and agriculture, fields in which Brazil possesses vast data resources, is highly valued in international research.

In addition, the country has characteristics that may favor technological experimentation. "Brazil has a continental-scale digital market operating under a relatively unified regulatory framework," Daniela highlights. This scenario may facilitate the adoption and large-scale testing of new artificial intelligence-based solutions.

Strengthening collaborations among universities, research centers, and startup ecosystems can expand innovation opportunities and accelerate the development of strategic technologies for science and education. •

Photo: RNP

Daniela highlights how AI is accelerating the transformation of the role of NRENs

EXPERIMENTATION *AND* MONITORING

Testbeds
The RNP National Multi-User Laboratory

MULTI-TECHNOLOGY INFRASTRUCTURE FOR RESEARCH AND INNOVATION

The National Multi-User Laboratory, operated by RNP, is an advanced, multi-technology infrastructure designed to support research, development, and innovation. It enables experimentation and validation in controlled, interconnected environments at a nationwide scale. Its mission is to provide academia, research centers, startups, and institutional partners with a distributed, flexible, and high-performance environment for experimentation in Information and Communication Technology (ICT).

The Laboratory supports testing and validation across a wide range of domains, including advanced networking, 5G/6G, IoT, cloud and edge computing, blockchain, cybersecurity, artificial intelligence, distributed applications, and emerging Internet architectures. By leveraging real-world infrastructure, it supports technical evaluations, proof-of-concept development, and performance analysis under realistic conditions.

By integrating infrastructure, specialized support, technical expertise, and nationwide coordination, the Laboratory expands opportunities for applied research and the development of skilled professionals. The initiative helps lower barriers to access complex environments, fosters collaboration among institutions, and strengthens RNP's role as a key enabler of science, education, and innovation in ICT in Brazil. •

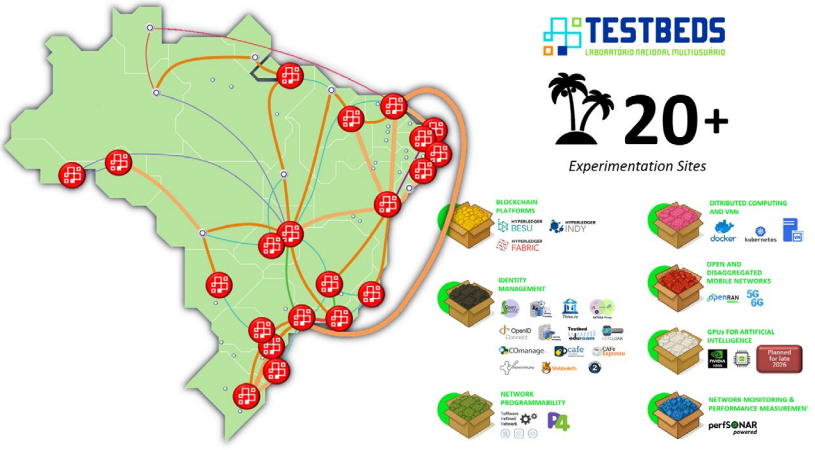
TECHNICAL ***INFORMATION***

GENERAL/ ACADEMIC COORDINATOR: Gustavo Neves Dias (RNP), *gustavo.dias@rnp.br*

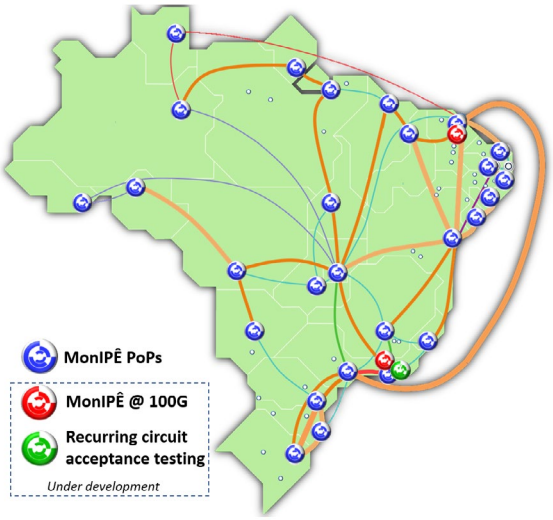
ASSISTANT COORDINATOR: Leandro Mondin (RNP), *leandro.mondin@rnp.br*

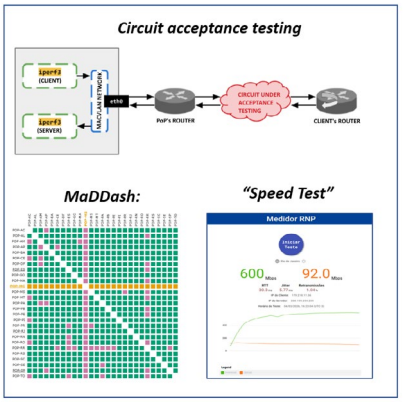
TEAM: Maria Elenice Pedrosa, Janssen Martins, Cesar Gama, Bruno Nascimento

QR CODE



TECHNOLOGIES, PEOPLE AND PURPOSE DRIVING RESEARCH, EDUCATION AND INNOVATION IN ICTS IN BRAZIL





MonIPÊ: The Ipê Network Certification Platform

CONTINUOUS EVOLUTION IN NETWORK QUALITY MEASUREMENT

TECHNICAL *INFORMATION*

GENERAL/ ACADEMIC COORDINATOR:
Gustavo Neves Dias (RNP), *gustavo.dias@rnp.br*

ASSISTANT COORDINATOR:
Marcos Felipe Schwarz (RNP), *marcos.schwarz@rnp.br*

TEAM:
Leandro Mondin, Daniel Neto, Elenice Pedrosa, Janssen Martins, Cesar Gama, João Bitencourt, Rafaela Fonseca, Robson Santos, Ronan Oliveira, Elder Storck, Thais Fernandes

MonIPÊ is RNP's platform for measuring and validating circuits that connect organizations to the RNP backbone. Initially used to assess latency and packet loss between Points of Presence (PoPs), the system has evolved into a reference tool for circuit validation in scenarios including new deployments, capacity upgrades, and provider changes. Its adoption has been driven by custom developments by the R&D team, which improved flexibility and enabled greater standardization and transparency in circuit certification.

Its core capabilities include the definition of standardized circuit acceptance workflows, automated scheduling and execution of tests, and the establishment of objective criteria for validating test results. The platform also provides comprehensive reporting and maintains a complete history of all testing and validation activities. Accessible through a simple, centralized web interface, MonIPÊ ensures end-to-end traceability, consistent result comparison, and improved operational efficiency.

These capabilities are enabled by RNP's technical expertise in perfSONAR and its active participation in the international consortium responsible for its maintenance and evolution. The 2026/2027 roadmap includes further enhancements, such as expanding support for link validation up to 10 Gbps across more PoPs, enabling continuous throughput assessment without impacting connected institutions, and supporting the certification of circuits up to 100 Gbit/s. •

ADVANCED MEASUREMENTS ENSURING NETWORK QUALITY

Technical Committee for Network Monitoring (CT-Mon)

CT-MON DRIVING RESEARCH WITH MONITORING DATA

Since 2011, the need to track technical and scientific changes in traffic monitoring has driven the activities of RNP's Technical Committee for Network Monitoring (CT-Mon). The group brings together researchers, network operations professionals, and representatives from the MonIPÊ service to explore technologies and formulate recommendations for monitoring services.

The infrastructure operated by RNP generates and stores network performance data. To transform this information into research opportunities, in 2025 the committee promoted the second RNP Backbone Monitoring Data Challenge, which brought together 15 teams from Brazilian universities, three of which were winners. The results were published in international conferences. Another important initiative is the organization of meetings with international researchers renowned in network measurement and monitoring, such as Lin Wang (Paderborn University), Fabrício Murai (WPI), Aruna Balasubramanian (SUNY Stonybrook), Luciana Kiffer (IMDEA, Spain), Amir Houmansadr (UMass-Amherst) e Adrian Perrig (ETH Zürich). In 2026, CT-Mon expanded its scope to address monitoring challenges identified by RNP, focusing on providing data access tools, standardizing metrics, and applying solutions that enable institutions to analyze traffic on their infrastructures in an interoperable way. The committee also organized the 3rd RNP Data Challenge. •

TECHNICAL
INFORMATION

GENERAL/ ACADEMIC COORDINATOR:
Antônio Augusto de Aragão Rocha (UFF), *arocha@ic.uff.br*

ASSISTANT COORDINATOR:
Daniel Otavio da *Cunha Cota (UFF), danielotavio@id.uff.br*

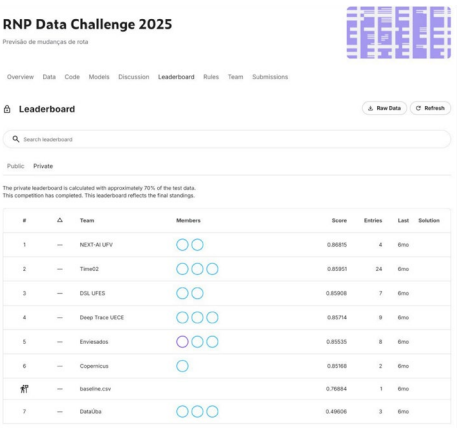
TEAM:
Gustavo Araújo (RNP) e José Ferreira de Rezende (RNP)

PARTNER
INSTITUTION

UFF

QR CODE

TRANSFORMING RNP MONITORING DATA INTO RESEARCH



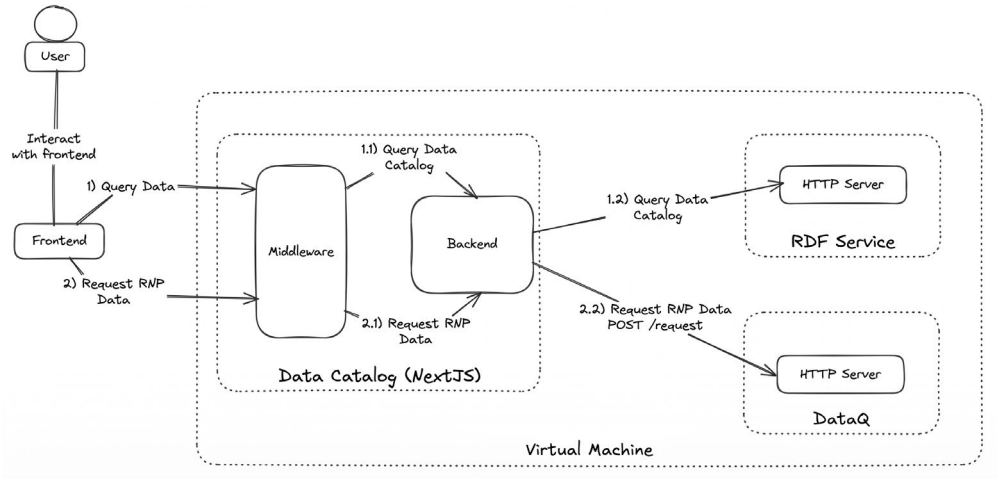
Network Data for Research

RNP TRANSFORMS OPERATIONAL DATA INTO ASSETS FOR SCIENCE

PROJECT CATALOGUES AND ANONYMIZES NETWORK DATA TO BOOST RESEARCH

RNP operates a complex infrastructure with national coverage that continuously generates massive volumes of operational data. These data represent a strategic asset still underutilized for scientific purposes, creating a gap between the potential generated by RNP's operation and the needs of the Brazilian research community in Artificial Intelligence and Data Science. This project aims to address this gap through specific and measurable objectives. The overall goal is to promote and facilitate the efficient use of network data for AI and Data Science, transforming operational data into a strategic asset for the scientific community.

In partnership with the Technical Committee for Network Monitoring (CT-Mon), the project seeks to: (i) catalog, process, and transfer a qualified information resource to RNP's Data Lakehouse platform; (ii) treat and anonymize network data in a structured and secure manner; (iii) develop and implement a centralized portal that enables researchers to discover datasets, access directories, and request data; (iv) promote the active dissemination of the repository through academic events, workshops, and conferences; and (v) validate the relevance of the data through the publication of scientific articles demonstrating their applicability in network research. These objectives expand RNP's role in the ICT research ecosystem, positioning it as a promoter of cutting-edge research in Brazil. •



TECHNICAL *INFORMATION*

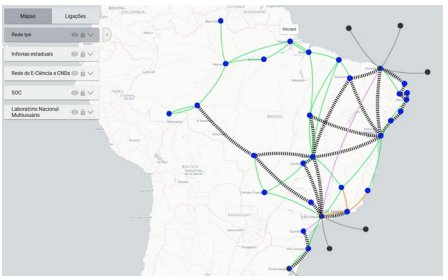
GENERAL/ ACADEMIC COORDINATOR:
Antônio Augusto de Aragão Rocha (UFF), *arocha@ic.uff.br*

ASSISTANT COORDINATOR:
Lucas Bondan (RNP), *lucas.bondan@rnp.br*

TEAM:
Marcos Laje, Daniel Oliveira, Nilson Damasceno, Rodrigo Chimelli, Marcelo Noberga, João de Morais, Gustavo Araújo, Marcos Schwarz, Daniel Neto, Filippo Venturini

PARTNER *INSTITUTION*

UFF



The Evolution of RNP Maps

INNOVATIONS FROM CHAMELEON MAP AND GREN MAP FOR ACADEMIC NETWORKS

Since 2022, the need to improve the reach, visibility, and communication of the various initiatives developed by RNP has driven the creation of the RNP Maps infrastructure. The project aims to offer a reference for visualizing projects, demonstrating their national scope and how their points of interest interconnect.

Currently, the initiative is divided into two main pillars: Chameleon Map and GREN Map. The Chameleon Map tool is already applied in various contexts, such as cybersecurity, blockchain, and RNP's own network. At present, Chameleon is undergoing a structural transformation: instead of operating as a standalone software, it is being adapted to a SaaS (Software as a Service) model. With the introduction of an administrative panel, users will be able to manage their maps with simplicity and autonomy. In addition, it adopts the Open Source model (open code), making its public code available on GitHub to encourage new contributors.

In parallel, we highlight GREN Map, which operates as a collaboration hub focused on understanding the topology of academic networks. The group is dedicated to standardizing, storing, and visualizing data, overcoming the historical fragmentation of this information and enabling different academic networks to describe their infrastructures in an interoperable way. •

RNP MAPS EVOLVE, BRINGING VISIBILITY, AUTONOMY AND COLLABORATION TO ACADEMIC NETWORKS

TECHNICAL ***INFORMATION***

GENERAL/ ACADEMIC COORDINATOR: Luciano Gaspary (UFRGS), *paschoal@inf.ufrgs.br*

ASSISTANT COORDINATOR: Gustavo Araújo (RNP), *gustavo.araujo@rnp.br*

TEAM: Gabriel Vassoler (RNP), Lisandro Granville (RNP), Eduardo Peretto (UFRGS), Leonardo Lauryel (UFRGS), Narciso Filho (UFRGS), Hugo Romão (UFRR)

PARTNER ***INSTITUTIONS***

RNP, UFRGS, UFRR e GNA-G

QR CODE

SCIERA: International Collaboration for a New Internet Architecture

A COLLABORATION NETWORK FOR EDUCATION AND RESEARCH IN SCION

It is now possible for educational and research institutions in Brazil to carry out experiments and research within the SCIERA (SCION Education, Research and Academic) network, a global infrastructure dedicated to the development and evaluation of the SCION (Scalability, Control and Isolation On Next-Generation Networks) architecture. The initiative brings together leading global research networks and institutions — such as GÉANT, Internet2, and KREONET/KISTI — creating a collaborative ecosystem that accelerates experimentation and innovation in next-generation networking.

Through the National Multi-User Laboratory, RNP has enabled Brazilian institutions to join the SCIERA network, allowing them to participate with their own SCION ASes in this global research environment. In this context, researchers and students can carry out studies directly on the SCION architecture, exploring topics such as inter-domain routing security, resilience to failures and attacks, multipath communication, path-aware networking, and data sovereignty..

SCIERA further enables international collaboration, supporting joint experiments and the development of solutions in resilient networking, cybersecurity, and low-latency applications. Through this initiative, RNP broadens Brazil's engagement in the global networking research landscape, fostering deeper integration with leading international efforts while contributing to the advancement of more secure, transparent, and resilient Internet architectures. •

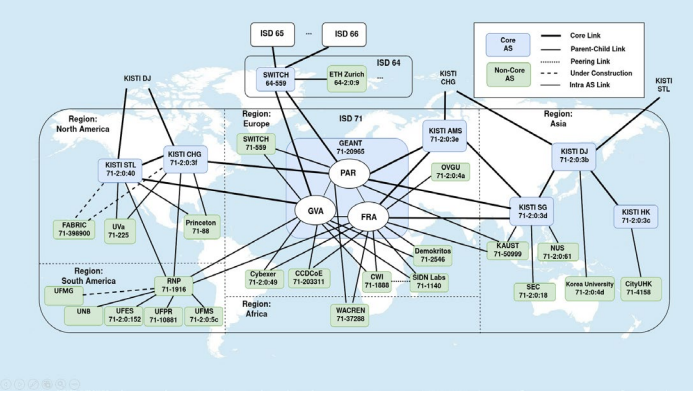
TECHNICAL ***INFORMATION***

GENERAL/ ACADEMIC COORDINATOR: Leandro Mondin (RNP), *leandro.mondin@rnp.br*

ASSISTANT COORDINATOR: Maria Elenice Pedrosa (RNP), *elenice.pedrosa@rnp.br*

TEAM: Janssen Martins (RNP) and Cesar Gama (RNP)

QR CODE



RNP CONNECTING BRAZILIAN INSTITUTIONS TO THE GLOBAL SCIERA RESEARCH NETWORK

E-SCIENCE

e-Science **Network**

HIGH-PERFORMANCE NETWORK FOR SCIENTIFIC DATA

The e-Science Network is a secure, high-performance digital infrastructure dedicated to research centers with advanced demands for processing, analysis, transmission, and storage of large volumes of data. Unlike the Ipê Network, the e-Science Network offers specialized policies and services for large-scale scientific data flows, with robust security measures.

This infrastructure primarily connects leading Science, Technology, and Innovation (ST&I) institutions, such as supercomputing centers, multi-user laboratories, and other data-intensive research environments. To enable this ultra-high-performance connectivity, RNP is upgrading its national optical infrastructure, making the backbone scalable to multiple 100 Gbps channels.

As a result, each participating institution will benefit from abundant bandwidth, optimized performance, and tailored services aligned with its specific demands. The construction of the e-Science Network is currently progressing on three funding streams. The main front is part of the Conecta structuring program (MCTI/FNDCT, prioritized under the New PAC 2023–2026), aimed at enabling the connection of 12 ST&I institutions.

In addition, a cooperation agreement with Petrobras will integrate six new research laboratories, while an agreement with the Ministry of Health will add five more by 2028. •

Ipê Network (RNP's primary internet backbone)	e-ScienceNetwork
The first Internet network in Brazil, evolving since 1992	Under construction, with expected completion in 2027
+1300 connected points	~20 connected points
With open Internet access	Without Internet access
Globally accessible from any Internet connection point	Accessible only through certified data transfer servers of participating institutions
Connectivity up to the institutional edge	Connectivity up to the scientific data storage server
Not optimized for data transfer; standard configuration for conventional applications (e-mail, video, online services, etc.)	Natively optimized for high-performance data transfers
Available to all organizations that are users of the RNP System	Requires compliance with specific security policies for an institution to join the network

TECHNICAL ***INFORMATION***

GENERAL/ ACADEMIC COORDINATOR:
Leandro Ciuffo (RNP), *leandro.ciuffo@rnp.br*

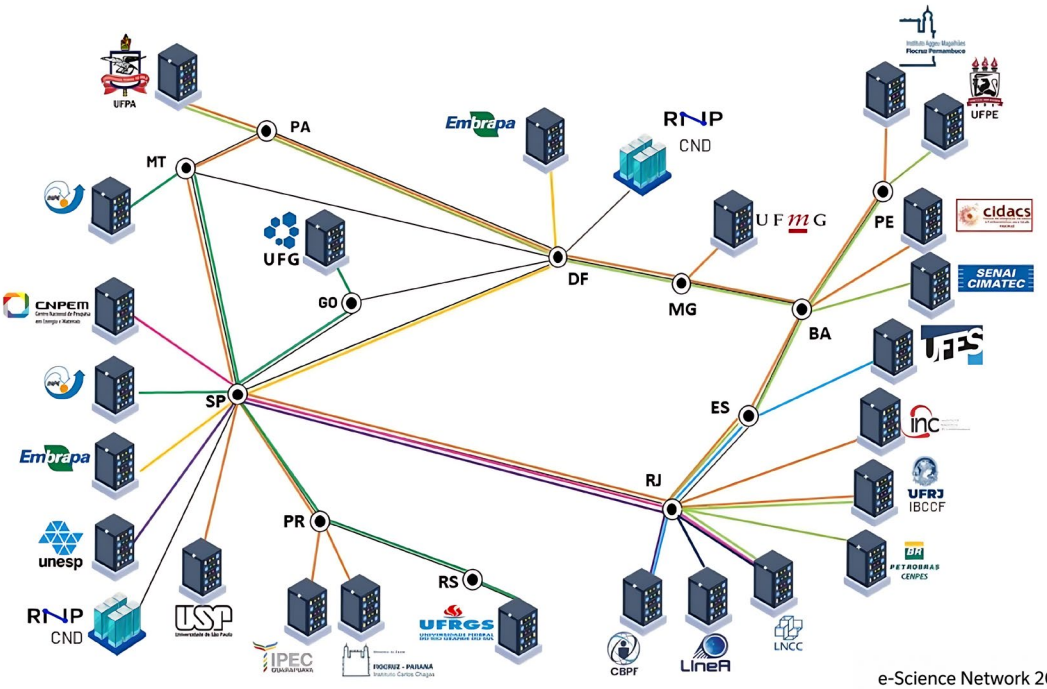
ASSISTANT COORDINATOR:
Débora Reis (RNP), *debora.reis@rnp.br*, Kesley Silva (RNP), *kesley.silva@rnp.br*

TEAM:
Jeferson Souza, Carlos Zilves, Edemir Matos, Luciana Ferreira, Ari Frazão, Aluizio Hazin, Allan Oliveira, Luiz Teixeira e Humberto Forsan

PARTNER ***INSTITUTIONS***

CBPF, CENPES, CNPEM, Embrapa, Fiocruz, INC, INPE, LIneA, LNCC, Senai-Cimatec, UFES, UFG, UFMG, UFPA, UFRGS, UFRJ, UNESP

QR CODE



HIGH-SPEED CONNECTIVITY DRIVING THE FUTURE OF SCIENTIFIC COLLABORATION

SCIENTIFIC DEMANDS AND CONNECTIONS

AGRICULTURE AND GENOMICS
EMBRAPA

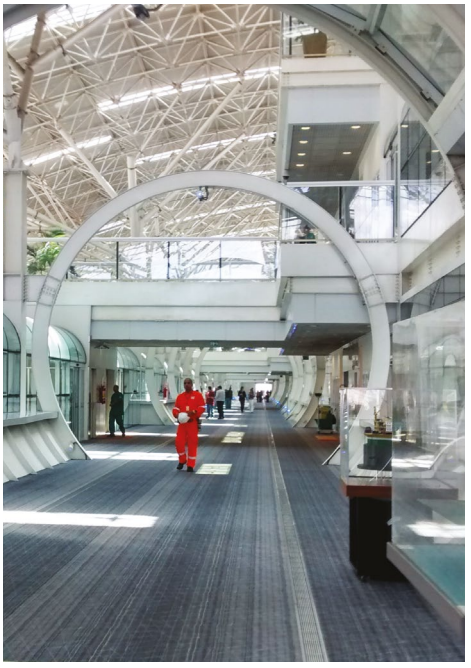
GENOMICS
UFMG – UFPA – UFRJ – IPEC – INC –
USP (SP and RP) – FIOCRUZ (PR, CIDACS and PE)

NANOTECHNOLOGY AND BIORENEWABLES
CNPEM – LNCC

COSMOLOGY
HIGH-ENERGY PHYSICS
ASTRONOMY
UNESP – CBPF – UFES
LineA – LNCC

GEOSCIENCE
LNCC – CENPES – SENAI-CIMATEC
UFRJ – UFPA – UFPE

METEOROLOGY
UFG – INPE
UFRGS – INPE



R&D and technology foresight in the e-Science network

OPTIMIZING LARGE-SCALE DATA MOVEMENT

Within the scope of the RNP-Petrobras cooperation agreement, the REPESQ project expands the e-Science Network to new ST&I institutions with growing demands for the movement of large volumes of geological, geophysical, and reservoir simulation data to Petrobras' research center (CENPES).

The program includes three research objectives across four work fronts. The first involves the development of an automated system for managing scientific workflows to enable remote access for CENPES researchers to supercomputers located at other institutions. The second front, with two complementary lines, focuses on the integrated optimization of hardware, network, and storage to support high-throughput data transfers over long distances—at 100G and prospecting toward 400G—emphasizing scalability, security, integrity, and fault mitigation.

The fourth front conducts technological foresight in Distributed Acoustic Sensing (DAS), identifying challenges to structure a future R&D program for processing and transmitting DAS-generated data in production environments. These combined objectives enable the development of new automated workflows for efficient large-scale data transfer to CENPES and among a group of eight ST&I institutions conducting joint research with Petrobras, consolidating the e-Science Network as a strategic cyberinfrastructure for Brazilian science. •

DEVELOPING SOLUTIONS FOR EFFICIENT MOVEMENT OF SCIENTIFIC DATA AMONG BRAZILIAN ST&I INSTITUTIONS

TECHNICAL *INFORMATION*

GENERAL/ ACADEMIC COORDINATOR:
Adriano da Silva Ferreira (RNP), *adriano.silva@rnp.br*

TEAM:
Antônio Tadeu, Vívian Medeiros, Welber Paraizo (LNCC), Fernando Redigolo, Vinicius Medeiros, Fernanda Lopes (USP), Aderson Farias (UFRN), Marcelo Bianchi (USP)

PARTNER *INSTITUTIONS*

CENPES, LNCC, USP, UFRN, SENAI-CIMATEC

Research data repositories **for the e-Science network**

A CASE STUDY WITH CLIMATOLOGICAL DATA FROM CEMPA-CERRADO/UFG

Throughout 2025, RNP, in partnership with UFG through its Center of Excellence in Environmental Studies, Monitoring and Forecasting of the Cerrado (CEMPA-Cerrado), advanced an initiative to improve the governance and management of climatological data in digital repositories.

The main motivation was to expand access and reuse of research data generated by scientific workflows within the e-Science Network. The initiative aimed to promote interoperability and facilitate the understanding of scientific information by researchers from different fields—not necessarily domain peers.

Initially, efforts to handle large volumes of data, characterized by complex matrices in scientific formats, resulted in infrastructure overload. As a solution, data transformation routines were implemented, generating derived datasets in smaller, structured formats, making them easier to consume for users without experience in digital repositories.

The enrichment of data derived from scientific workflows broadened access while maintaining scientific rigor and enabling data reuse in digital repositories by researchers or through AI-based analytical tools. Access to climatological data in Goiás was democratized, eliminating the need for specialized scientific tools.

This case study is expected to be expanded to other domains and ST&I institutions within the RNP e-Science Network, allowing a broader set of users to benefit from improved data governance and management in digital repositories. •

DIGITAL REPOSITORIES FOR IMPROVED GOVERNANCE AND MANAGEMENT OF SCIENTIFIC DATA

TECHNICAL ***INFORMATION***

GENERAL/ ACADEMIC COORDINATOR: Prof. Dra. Laura Vilela Rodrigues Rezende (UFG), *laura_rezende@ufg.br*

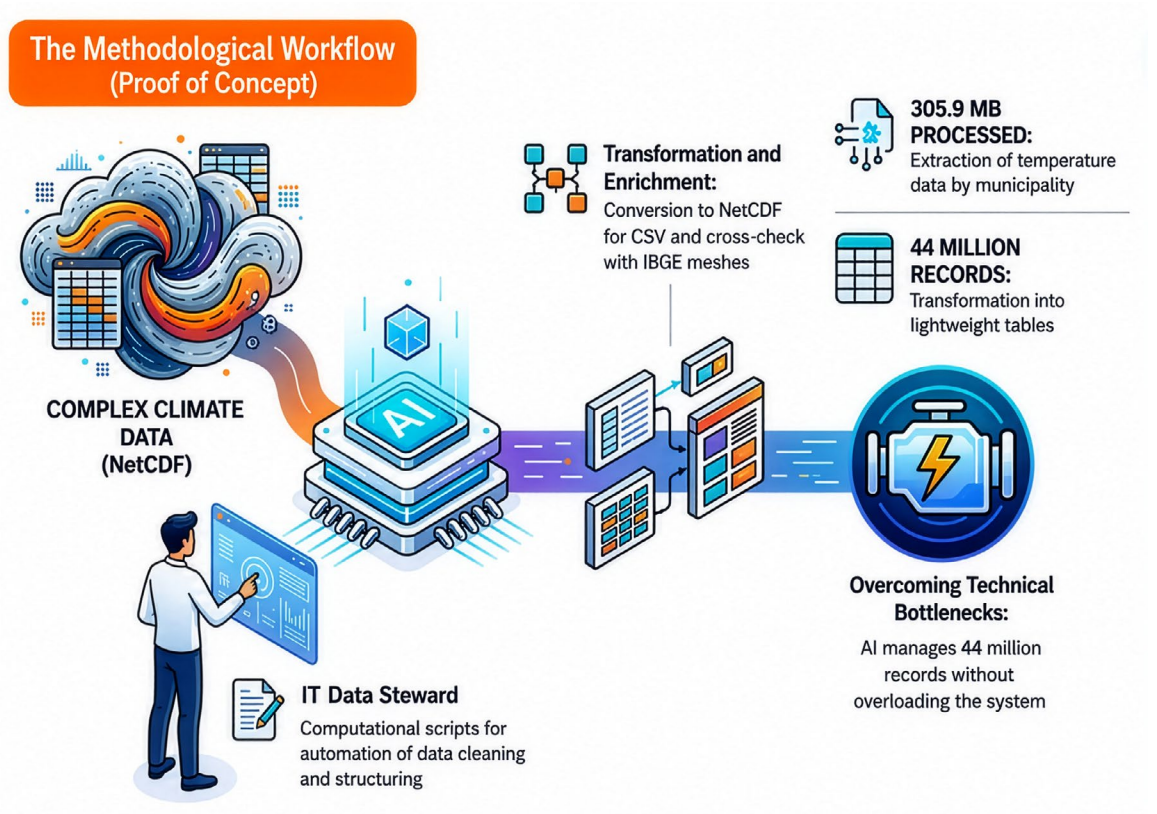
TECHNICAL COORDINATOR: Prof. Dra. Kátia Kelvis (UFG), *katiakelvis@ufg.br*

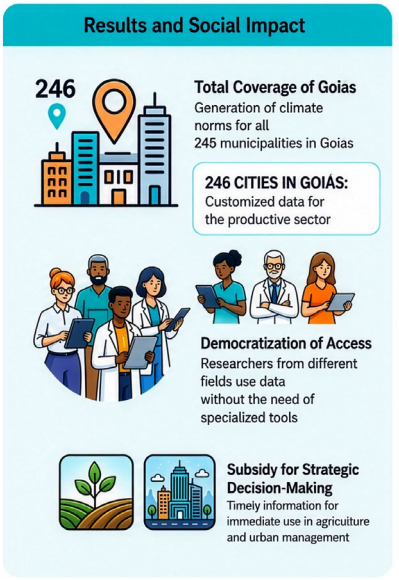
R&D COORDINATOR: Carolina Howard Felicissimo (RNP), *carolina.felicissimo@rnp.br*

TEAM: Angel Chovert, Anne Oliveira, Breno de Lima, Geisa Ribeiro

AI in Open Science: From Data Curation to Information Democracy

Methodological Workflow and Results from the Proof of Concept (PoC) in Complex Climate Data





R&D for identity and access management in the e-Science network

PROOF OF CONCEPT AND CASE STUDY WITH ST&I INSTITUTIONS

Research infrastructures increasingly rely on secure and interoperable mechanisms for user authentication and authorization. In many cases, research collaborations involve participants from multiple institutions and even companies, increasing the complexity of access control.

Therefore, an environment is required to manage the entire lifecycle of Virtual Organizations—a temporary logical grouping of individuals, often from different institutions, collaborating around a project. This environment enables researchers from multiple institutions to access services and collaborative workspaces using only the credentials from their home institution.

Based on this need, and aligned with international initiatives, the Working Groups involved in this project are analyzing existing platforms (CILogon and MyAccessID) and proposing Identity and Access Management (IAM) solutions tailored to the context of e-Science Network institutions.

Among the evaluated options, an architecture integrating CILogon with modern authentication protocols, such as OpenID Connect (OIDC), stands out, along with a proof of concept based on the AARC Blueprint Architecture, widely adopted by the international community to organize federated identity services.

In addition, a proof of concept is being developed to integrate Globus, a solution designed to facilitate and automate data transfer workflows between institutions within the e-Science Network. •

CILogon

TECHNICAL ***INFORMATION***

PRINCIPAL INVESTIGATOR:
Walter Priesnitz Filho (UFSM), *walter.filho@ufsm.br*

TEAM:
Heitor Scalco Neto, Renato Preigschadt de Azevedo, José Carlos Lacerda Lopes Neto, Gustavo Peretti, Gabriel Denarde

MYAccessID

TECHNICAL ***INFORMATION***

PRINCIPAL INVESTIGATOR:
Edelberto Franco Silva (UFJF), *edelberto.franco@ufjf.br*

ASSOCIATE RESEARCHER:
Bruno Dembogurski, *bruno dembogurski@ufrrj.br*

TEAM:
Allan Marcelino, Leonan Louvem, Pedro Henrique Silva, Bruno José Dembogurski

SOLUTIONS IN IAM: CILOGON, MYACCESSID AND GLOBUS

COLLABORATION *AND THE FUTURE*

RNP & Startups Collaboration Network: **experimentation and innovation**

RNP'S PROOF OF CONCEPT MODEL BRIDGES RESEARCH, STARTUPS, AND ORGANIZATIONS CONNECTED TO THE RNP SYSTEM

The RNP & Startups Collaboration Network was created to strengthen the connection between research outcomes developed within RNP's R&D programs and the innovation ecosystem, supporting startups emerging from research groups and projects.

One of the initiative's recent advances is the implementation of Proofs of Concept (PoCs), which enables the testing of technological solutions in real-world environments alongside organizations connected to the RNP System. These experiments help validate technologies, understand institutional needs, and generate evidence for the adoption or scaling of solutions.

A notable example is the PoC conducted with the startup Reabnet, which evaluated a gamified digital care model for elderly patients in partnership with the Hospital das Clínicas of the Federal University of Uberlândia and Unimed Uberlândia. The results demonstrated strong participant engagement and significant improvements in clinical and functional indicators, highlighting the solution's scalability potential.

Other PoCs are currently on going, including projects in MetaHealth, in partnership with UFMG and Unifesp, as well as an international collaboration between the startup RingO and RENU, Uganda's research and education network. The initiative also promotes specialized mentoring, supports fundraising efforts, and fosters connections with early adopters, expanding RNP's role as a platform for technological experimentation and contributing to transforming research outcomes into innovative solutions with social and economic impact.

TECHNICAL ***INFORMATION***

MANAGER:
Rafael Valle (RNP),
rafael.valle@rnp.br

COORDINATOR:
Ana Geórgia Damasceno Barbosa (RNP),
ana.barbosa@rnp.br

TEAM:
Felipe Nascimento, Henrique Ferraz, José Henrique Dieguez, John Forman

QR CODE

POCS ARE CONNECTING STARTUPS, RESEARCH, AND ORGANIZATIONS TO VALIDATE INNOVATIVE SOLUTIONS

Presente! **Your Intelligent Classroom**

CLASSROOM ENGAGEMENT ANALYZED THROUGH AI AND 5G TO SUPPORT EDUCATION

The Presente! - Your Intelligent Classroom project explores the use of artificial intelligence and computer vision to understand student engagement in the classroom and support improvements in the learning process. Coordinated by RNP, and developed in conjunction with Inatel and UFRJ, the solution is implemented in an Inatel classroom. It operates over a private 5G network, ensuring low latency, high reliability, and near real-time processing capacity.

The system architecture leverages edge computing to process multimodal data collected from multiple cameras in the classroom. Through machine learning models and computer vision, the platform identifies patterns of behavior, interaction, and participation throughout activities, enabling the estimation of collective engagement levels.

Analyses are conducted based on aggregated and anonymized data, without individual identification of students, preserving participants' privacy. Processing occurs in real time, without the need for permanent image storage, ensuring greater security in data handling.

From these analyses, the system generates indicators that can support professors and educational managers in evaluating pedagogical strategies and understanding classroom participation dynamics. In addition to engagement analysis, the project also investigates complementary applications, such as intelligent access control and automated attendance tracking through facial recognition, contributing to the modernization of academic management. •

TECHNOLOGY TRANSFORMS CLASSROOM DATA INTO EVIDENCE TO IMPROVE LEARNING

TECHNICAL ***INFORMATION***

GENERAL/ ACADEMIC COORDINATOR:
José Ferreira de Rezende (RNP), *jose.rezende@rnp.br*

ASSISTANT COORDINATOR:
Clayton Reis da Silva (RNP), *clayton.reis@rnp.br*

TEAM:
RNP: Iara Machado, Leonardo Ribeiro
UFRJ: Sergio L. Netto, Eduardo da Silva, Thadeu Dias
INATEL: Cristiani Guimarães, Douglas Pereira, Murilo Lopes, Ana Serafim

PARTNER ***INSTITUTIONS***

INATEL and UFRJ

CT-CDIA: **advancing R&D, infrastructure and innovation in AI**

CONNECTING UNIVERSITIES AND R&D CENTERS IN THE NEW AI ERA

The world is experiencing a new technological era driven by advances in artificial intelligence, which is rapidly transforming science, industry, and education, impacting all sectors of society. As in the early days of computer networks, Brazil faces significant challenges, such as the lack of adequate infrastructure for AI.

At the same time, the training of human resources capable of understanding, developing, and using AI technologies responsibly remains insufficient. The rapid evolution of this field is driven by trends such as the emergence of agents capable of making autonomous decisions or acting in a coordinated manner.

RNP, which connects Brazilian institutions and provides essential services for research and education, can play a strategic role by offering AI research services that stimulate collaboration and innovation. An initiative aligned with this effort is CT-CDIA - Technical Committee on Data Science and Artificial Intelligence.

The committee will promote lectures, workshops, and panels with experts from Brazil and abroad to discuss emerging AI technologies and their potential benefits for society. Its objectives include identifying the needs of the community for research, education, and implementation, as well as discussing how RNP can develop platforms to evaluate AI systems under realistic conditions, integrating infrastructure and distributed data across the country. These actions aim to strengthen Brazil's capabilities in advanced digital technologies.

TECHNICAL ***INFORMATION***

GENERAL/ ACADEMIC COORDINATOR:
Edmundo de Souza e Silva (UFRJ), *edmundo@land.ufrj.br*

TEAM:
Altigran Soares da Silva, Andre Carlos Ponce de Leon, Claudia Bauzer Medeiros, Flávio Rech Wagner, Teresa Ludermir, Wagner Meira

RNP HAS BEEN ESSENTIAL TO THE DEVELOPMENT OF NETWORKS AND CAN PLAY A STRATEGIC ROLE IN THE AI ERA

Technical committee on identity and access management (CT-GId)

TECHNOLOGY FORESIGHT IN IDENTITY MANAGEMENT

Established by RNP in 2010, the committee aims to develop technical recommendations and project a future vision for RNP in the fields of Identity and Access Management (IAM) and Authentication and Authorization Infrastructures (AAI). Participation in CT-GId is open to specialists and professionals working in related areas, fostering technical diversity and expanding contributions to the sector.

The committee operates in annual cycles, tracking key developments from academia and industry. It promotes initiatives such as lectures, technical studies, and the development of proof-of-concept projects.

The future vision report, updated every two years, identifies trends that may evolve current services, drive new services, or shape business models for RNP in the field of identity and access management. The 2025 report highlights trends such as decentralized digital identity, agentic identity, identity for workload, and zero-trust architectures.

In 2026, the committee is working on a new format for the vision report, including an executive summary version and a more detailed version to support academia and RNP in identifying trends in the field. •

DECENTRALIZED DIGITAL IDENTITY AND AGENTIC AI ARE KEY TRENDS IN IDENTITY MANAGEMENT

TECHNICAL ***INFORMATION***

GENERAL/ ACADEMIC COORDINATOR:
Emerson Ribeiro de Mello (IFCS), *mello@ifsc.edu.br*

COORDINATOR:
Shirlei Aparecida de Chaves (IFSC), *shirlei.chaves@ifsc.edu.br*

TEAM:
Secretary:
Fiterlinge Martins de Sousa (RNP)

QR CODE

OPEN NET WORKING

Digital Twins of RNP's Networks

VIRTUAL LABORATORIES FOR THE DIFFERENT NETWORKS OF THE RNP SYSTEM

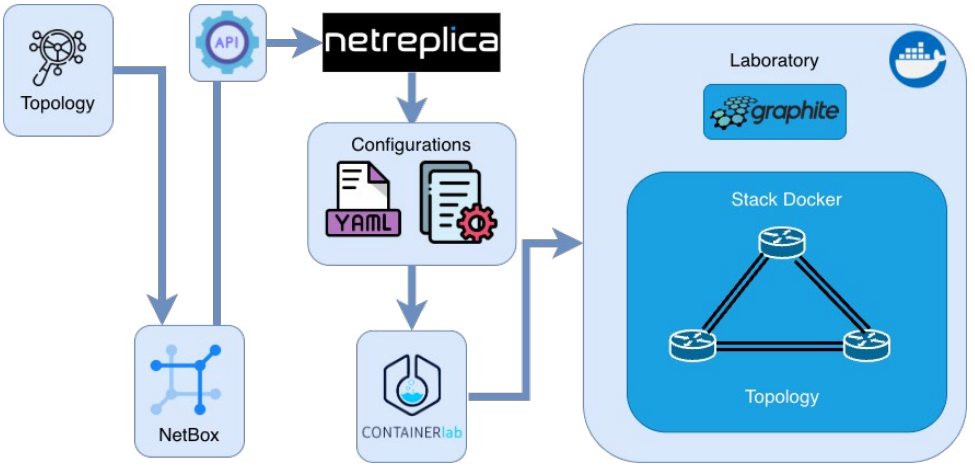
COLLABORATIVE EVOLUTION OF RNP NETWORKS BETWEEN OPERATORS AND RESEARCHERS

This initiative aims to create virtual network laboratories using digital twins of the different networks within the RNP System, such as the national backbone (Ipê Network) and metropolitan networks.

Leveraging the expertise of network analysts from RNP Points of Presence and academic researchers, open tutorials are created to explore and disseminate new methodologies, paradigms, and network tools, relevant even for real-time network operations, research, and experimentation.

In 2026, the project is expected to focus on end-to-end network services, serving as an environment for development, testing, and training of: 1) network infrastructure monitoring systems; 2) practical scenarios applying the use of AI in networks; and 3) dynamic end-to-end circuit solutions for metropolitan networks, spanning PoPs and the Ipê Network.

The main impact is enabling the evolution of RNP networks toward a collaborative model, with teams going beyond operational roles, facilitating the execution of R&D projects in partnership with academia, and enabling the replication of environments in real-world topologies for technology transfer and knowledge exchange between R&D and production teams. •



TECHNICAL ***INFORMATION***

GENERAL/ ACADEMIC COORDINATOR: Marcos Schwarz (RNP), *marcos.schwarz@rnp.br*

ASSISTANT COORDINATOR: Gustavo Araújo (RNP), *gustavo.araujo@rnp.br*

TEAM:
UFRR/PoP-RR: Kaio Guilherme
UFRA/PoP-PA: Eduardo Castro
PoP-RJ: Rafael Brandão
UFC/PoP-CE: Felipe Anjos
RNP: Lucas Borges

QR CODE

Brazil is accelerating toward 6G with state-of-the-art computing infrastructure and artificial intelligence

HPC INFRASTRUCTURE EXPANDS BRAZILIAN RESEARCH IN 6G NETWORKS

Launched in 2021, the Brasil 6G Program has established itself as a strategic initiative to position the country not only as a consumer, but also as a developer of technologies and standards for the next generation of mobile networks

Funded by MCTI through RNP's Advanced Internet R&D program, the project is being carried out in partnership with Inatel and CPQD. It is currently in its third phase, focused on integrating artificial intelligence and developing the 6G Experimentation Platform.

To support this stage, the initiative includes investments of more than R$5 million in cutting-edge equipment. This infrastructure includes software-defined radios, protocol and spectrum analyzers, as well as an advanced high-performance computing (HPC) solution with AI capabilities.

With these resources, it becomes possible to validate radio access technologies and core network components, enabling researchers to process large volumes of data to train machine learning models for 6G networks

Phase 3 has already brought together around 144 professionals and 77 scholarship holders, generating meaningful results in scientific output, software development, patent filings, talent development, and prototype creation. By uniting leading institutions such as UFPA, UFC, Unicamp, UFSC, UFRJ, Unisinos, and UFG, the Brazil 6G Program strengthens national scientific collaboration and prepares the country for the challenges of an increasingly connected future. •

Brasil 6G

PHASE 3 FOCUSES ON HPC AND AI TO STRENGTHEN TECHNOLOGICAL SOVEREIGNTY AND NATIONAL INNOVATION IN 6G

TECHNICAL *INFORMATION*

GENERAL/ ACADEMIC COORDINATOR: Fernando N. N. Farias (RNP), *fernando.farias@rnp.br*

PROJECT COORDINATOR: Bárbara Évellyn (RNP), *barbara.santos@rnp.br*

TEAM: Michelle Wangham, Bruno Ciro, Diego Abreu, José Rezende, José Brito, Daniely Gomes, Luciano Mendes, Juliano Ferreira

PARTNER *INSTITUTIONS*

UFG, UFC, UNISINOS, UFSC, UFPA, UFRJ, UNICAMP, INATEL,CPQD

QR CODE

OpenRAN@Brasil **Program**

OPEN INFRASTRUCTURE, INNOVATION, AND COLLABORATION IN MOBILE NETWORKS

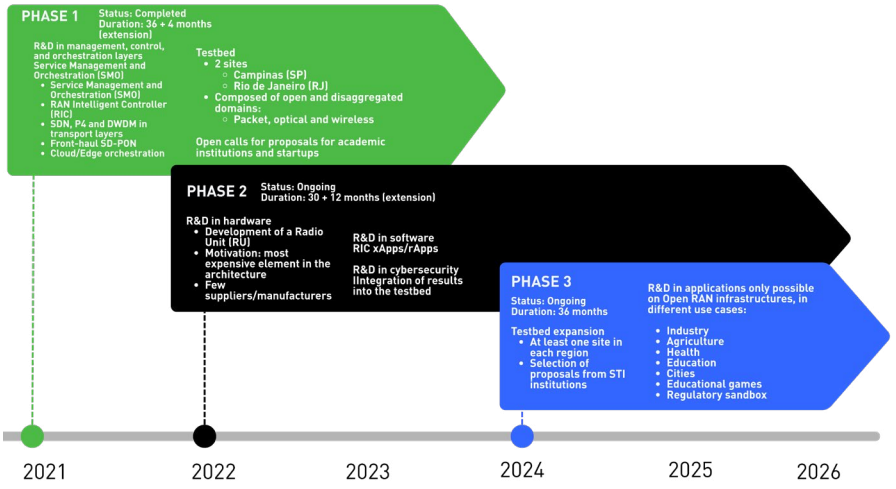
The OpenRAN@Brasil Program has established itself as the leading national initiative for the research, development, and validation of Open RAN technologies in realistic and interoperable environments. Structured as a multi-institutional testbed, the program brings together universities, research centers, and industry partners to accelerate the maturity of open solutions for mobile networks.

Throughout its evolution, organized into three complementary phases, OpenRAN@Brasil has advanced the implementation of a laboratory infrastructure for integrating radio modules, control software, orchestration, and management, addressing concrete challenges in interoperability, performance, and automation.

The environment enables experimentation with disaggregated architectures, end-to-end integration testing, and the evaluation of use cases aligned with national demands. More than a technological platform, the program acts as a catalyst for the development of specialized human resources, international collaboration, and the strengthening of strategic competencies.

By promoting open standards and collaborative ecosystems, OpenRAN@Brasil contributes to increasing national competitiveness and strengthening technological sovereignty in mobile networks. •

NATIONAL TESTBED DRIVES INNOVATION AND SOVEREIGNTY IN OPEN RAN NETWORKS



TECHNICAL *INFORMATION*

INTEGRATION COORDINATOR:
Lucas Bondan (RNP), *lucas.bondan@rnp.br*

PROJECT COORDINATOR:
Leonardo Carvalho Ribeiro (RNP), *leonardo.ribeiro@rnp.br*

TEAM:
Fernando Farias, Gustavo Araújo, Daniel Marques, Elaine Barioni, Érico Bastos, Francisco Portelinha, Fábio Takaki

PARTNER *INSTITUTIONS*

CPqD, Inatel, Eldorado, UFG, UnB, UFRGS, UNISINOS, UFPA, UFRJ, UFCG, UFF, UFSCAR, UFRN, PUCRS, UFCSPA

QR CODE

BLOCK CHAIN

Brazilian Blockchain Observatory: a model for scientific dissemination

DATA CURATION, COMMUNITY ENGAGEMENT, AND PUBLIC INTEREST

The Brazilian Blockchain Observatory has been consolidating itself as an institutional model for scientific dissemination based on data curation, community engagement, and a focus on public-interest information. From April 2025 to March 2026, the platform has mapped more than 580 blockchain initiatives; indexed approximately 2.2 million scientific outputs—including theses, dissertations, and articles—; organized more than 10 meetings of the Blockchain Specialists Community; reported around 130 use cases; and reached 1,700 users on LinkedIn. The Observatory team has interviewed 11 researchers in the field, established five strategic partnerships, and participated in 13 events to promote initiatives and objectives related to strengthening the blockchain ecosystem in Brazil. Overall, knowledge production and data governance efforts have resulted in seven publications, including articles, technical reports, and scientific dissemination materials. In this way, the Observatory goes beyond traditional information dissemination models and establishes itself as a replicable methodology, primarily based on the mediation and co-production of knowledge. In the near future, the Observatory will expand its scientific output indicators and strengthen its focus on the connections generated within the community, enhancing visibility and collaboration among stakeholders in science, technology, and innovation, in alignment with Brazil's national innovation agenda. •

THE OBSERVATORY WILL EXPAND INDICATORS AND STRENGTHEN FOCUS ON NETWORKED CONNECTIONS

TECHNICAL ***INFORMATION***

EDITORIAL COMMITTEE: Bárbara Evellyn and Larriza Thurler (RNP); Luana Cruz (jornalista); Glauber Gonçalves (UFPI); Ismael Ávila e Silvia Marion (CPQD), *contato@observatorioblockchain.org.br*

PARTNER ***INSTITUTIONS***

Ibict/BrCris, iColab, Polkadot Education, Cardano Academy

QR CODE

Iliada: Integrating Distributed Ledgers, Infrastructure and Decentralized Applications

RESEARCH, EXPERIMENTATION, AND INNOVATION IN BLOCKCHAIN

Coordinated by Softex and executed by RNP and CPQD under the PPI Softex Program, the Iliada Project launched three public calls and selected 13 working groups and four startups to develop applications and expand scientific knowledge in blockchain. R&D activities mobilized 106 fellows, in addition to the RNP team. The solutions were validated in a multi-platform testbed, enabling researchers and developers to experiment with different blockchain platforms and architectures in a collaborative environment. The project also developed the EasyLedger tool, which facilitates and automates the creation of blockchain networks in experimental environments. The infrastructure includes eight dedicated servers hosted at RNP Points of Presence distributed across the country, totaling a computing capacity exceeding 500 CPU cores, more than 2 TB of RAM, and approximately 40 TB of storage. This setup provides a robust infrastructure for large-scale experimentation. Another key outcome of Iliada is the Brazilian Blockchain Observatory, a platform that curates data, research, and initiatives, supporting the mapping and visibility of the blockchain ecosystem in Brazil. The following section highlights some of the project's initiatives. •

R&D ACTIVITIES MOBILIZED 106 FELLOWS FROM 23 INSTITUTIONS, IN ADDITION TO THE RNP TEAM

TECHNICAL *INFORMATION*

GENERAL/ ACADEMIC COORDINATOR:
Leandro Ciuffo (RNP), *leandro.ciuffo@rnp.br*

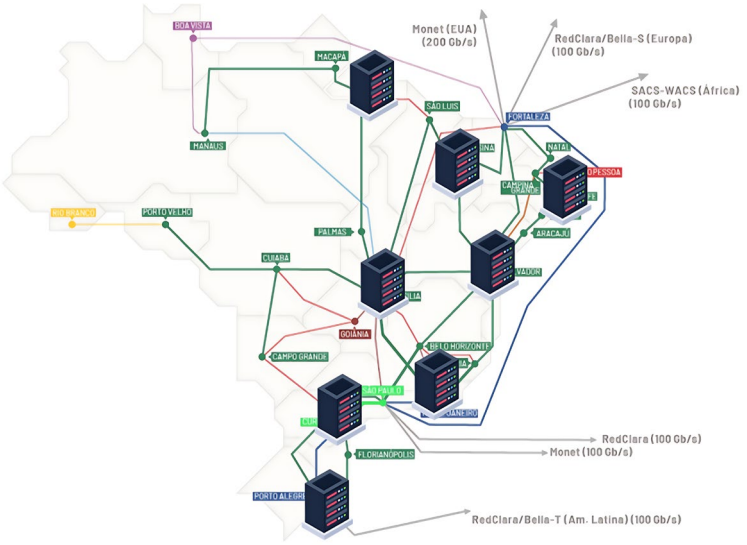
ASSISTANT COORDINATOR:
Bárbara Évellyn (RNP), *barbara.santos@rnp.br*

TEAM:
Iara Machado, Michelle Wangham, Ana Landi, Estefânia Arata, Giovana Barbosa, Kauane Cordeiro, Larissa Salles, Larriza Thurler, Luiz Folly, Marcos Schwarz, Pedro Neves, Reinaldo Gomes

PARTNER *INSTITUTIONS*

CPQD, UFPR, UFPA, UFC, UFF, IFBA, IFPI, UFPI, Unioeste, PUC-MG, UnB and Amachains

QR CODE



Researchers from
23 universities

Over
100 fellowships
supporting RD&I

2 fellowships
in science communication

13 research
groups using
the testbed

5 startups involved

CarbonID

A PLATFORM FOR MANAGING AND TRACKING DIGITAL ASSETS

CarbonID is a technological platform designed to enhance transparency, traceability, and reliability throughout the lifecycle of projects and digital assets, such as carbon credits. The solution integrates emerging technologies, including blockchain, smart contracts, and Decentralized Digital Identity (DID), enabling the registration, validation, and tracking of all stages associated with the creation, certification, and use of assets. By leveraging blockchain, the platform ensures immutable and auditable records of project data and metadata, creating a trusted repository that helps reduce inconsistencies, strengthen trust among ecosystem participants, and support auditing and verification processes across different institutions. Additionally, the adoption of DID mechanisms enables the authentication and accountability of entities involved in platform operations, such as project developers, auditors, certifiers, and buyers, ensuring that each record is linked to verifiable digital identities. The platform also provides tools to monitor the history and status of projects and assets, promoting greater visibility, governance, and data integrity. In this way, CarbonID contributes to strengthening credibility and transparency in carbon markets and other traceable digital asset ecosystems.

CarbonID

CARBONID INTEGRATES BLOCKCHAIN AND DID TO ENSURE TRACEABILITY OF ENVIRONMENTAL ASSETS

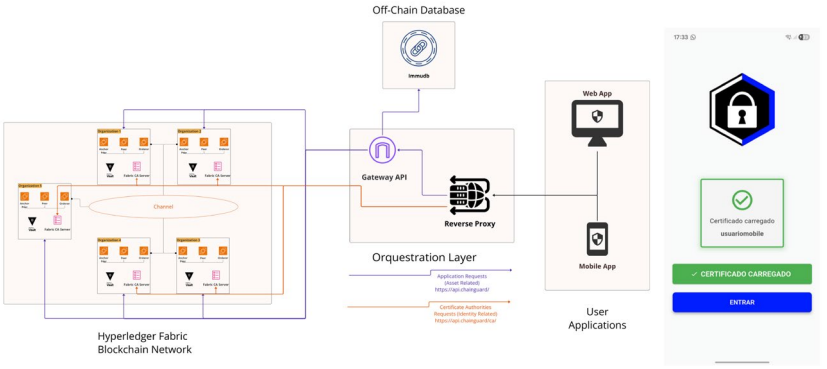
TECHNICAL ***INFORMATION***

GENERAL/ ACADEMIC COORDINATOR:
Leobino Nascimento Sampaio (UFBA), *leobino@gmail.com*

ASSISTANT COORDINATOR:
Silvio José de Queiroz Pereira (UFBA), *silvio.queiroz@gmail.com*

TEAM:
Leobino Sampaio, Silvio Pereira, Osvaldo Santana Filho, Igor Santos, Anderson Carvalho, Ederson Assunção

QR CODE



A BLOCKCHAIN-BASED CHAIN OF CUSTODY SOLUTION

ChainGuard: a solution for preserving the chain of custody of digital evidence

The concept of chain of custody was incorporated into the Brazilian legal framework through Law No. 13,964/2019, which introduced provisions in the Criminal Procedure Code to ensure the traceability, integrity, and authenticity of evidence used in investigations and judicial proceedings. In this context, it is essential to ensure that digital evidence is preserved and documented throughout its entire lifecycle. To address these requirements, the ChainGuard project developed a blockchain-based digital infrastructure for managing the chain of custody of digital evidence, replicating operational workflows used by public security agencies, as well as supporting applications for collection, recording, and auditing of evidence. The solution is composed of three main components: user applications, including a mobile application for field data collection and a web application for administrative management; an orchestration layer responsible for integrating and controlling system requests; and a permissioned blockchain network based on Hyperledger Fabric, used as an immutable transaction ledger. Complementing the system, an off-chain immutable database stores evidence and metadata. By integrating distributed records, digital signatures, and cryptographic traceability, ChainGuard demonstrates the potential of blockchain technology to strengthen the integrity and auditability of digital evidence chains of custody. •

BLOCKCHAIN ENHANCES THE RELIABILITY OF DIGITAL EVIDENCE CHAIN OF CUSTODY IN BRAZIL

TECHNICAL *INFORMATION*

GENERAL/ ACADEMIC COORDINATOR: Renato Hidaka Torres (UFPA), *renatohidaka@ufpa.br*

ASSISTANT COORDINATOR: Roberto Samarone (UFPA), *rsa@ufpa.br*

TEAM: João Santos, Kevin Cruz, Sainy Dias Antonio, Yasmim Yosano, Roberto Samarone, Renato Hidaka Torres

PARTNER *INSTITUTION*

Public Prosecutor's Office of the State of Pará

QR CODE

Enhancing the production chain and strengthening **food security in Brazil**

BLOCKCHAIN SERVING FAMILY FARMING

Family farming accounts for 77% of agricultural establishments in Brazil, playing a strategic role in ensuring food reaches the population's table. Despite its relevance, the sector faces the challenge of balancing tradition and innovation to meet regulatory requirements such as Joint Normative Instruction INC 02/2018 (MAPA/ANVISA).

In this context, the Smart Agro RAF Working Group investigates the use of blockchain, smart contracts, and trust infrastructure for agri-food traceability in family farming. The project is based on a decentralized, interoperable, and open-source architecture that ensures producers retain sovereignty over their data, reducing dependency on centralized platforms and associated costs, often incompatible with the realities of small-scale farmers. In this way, the initiative contributes to advances in data governance, origin certification, and digital inclusion, while fostering the development of scalable traceability solutions applicable to public policies and distributed supply chains. The solution meets the regulatory requirements of INC 02/2018, which governs traceability of fresh vegetables. Validated through the Family Farming Traceability Program (PROAF), the platform is currently being implemented at Federal University of the Pampa (UNIPAMPA) in Alegrete (RS) and is available online (proraf.com.br). Its open architecture enables other traceability systems to adopt its components, supporting the dissemination of accessible, interoperable, and regulation-compliant solutions. •

AN OPEN AND FLEXIBLE TECHNOLOGY TO ENABLE TRACEABILITY AND STRENGTHEN FOOD SECURITY

Smart Agro RAF by Proraf

TECHNICAL ***INFORMATION***

GENERAL/ ACADEMIC COORDINATOR:
Rodrigo Brandão Mansilha (Unipampa), *mansilha@unipampa.edu.br*

TEAM:
Diego Kreutz, Roben Lunardi, Henrique Fan, Rafael Nogueira, Bruno Neves

PARTNER ***INSTITUTION***

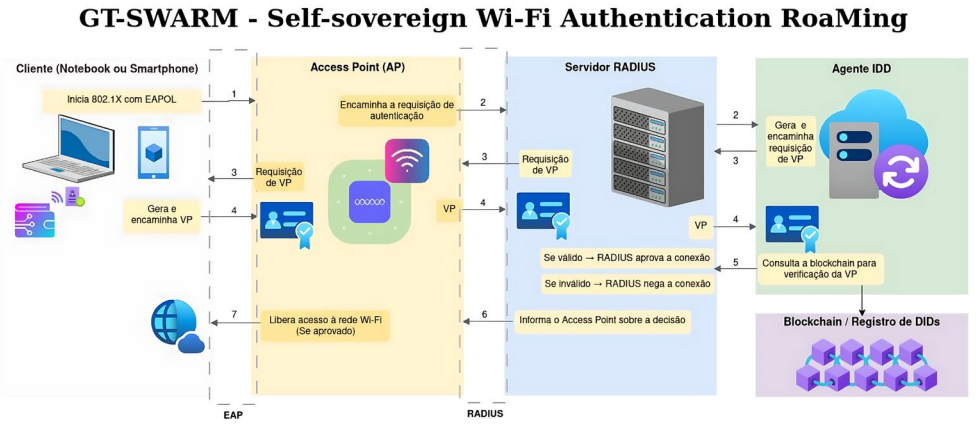
IFRS

QR CODE

SWARM **Working Group**

SELF-SOVEREIGN WI-FI AUTHENTICATION ROAMING

The SWARM Working Group (Self-sovereign Wi-Fi Authentication Roaming) emerged in response to concerns about user privacy in Internet service access. New Decentralized Digital Identity (DID) technologies enable individual ownership of credentials for service authentication. In this context, the project developed a Wi-Fi authentication method based on IEEE 802.1X, using the EAP protocol, integrated with Hyperledger Indy and Cardano blockchain frameworks, aiming for interoperability with eduroam. The solution adopts verifiable credentials (VCs), stored in users' digital wallets, and supports the issuance of verifiable presentations (VPs) on demand for authentication. The software developed includes an EAP-DID module within a reference EAP implementation (hostap/eapol), as well as a proxy component (Hermes proxy) for communication between the module and the identity provider. An architecture was also designed to integrate system components and user data models, enabling decentralized authentication. System performance was evaluated against the EAP-MD5 method, with an average authentication time increase from 2 to 4 seconds. The project still faces challenges in areas such as standardization of the new EAP method, implementation of supplicants, integration with digital wallets, deeper performance evaluations, and governance models for VC issuance. Nevertheless, it contributes to a more secure ecosystem aligned with privacy and user digital sovereignty. •



THE SWARM WORKING GROUP ENABLED 802.1X AUTHENTICATION WITH DECENTRALIZED DIGITAL IDENTITIES

TECHNICAL ***INFORMATION***

GENERAL/ ACADEMIC COORDINATOR: Carla Merkle Westphall (LRG – UFSC), *carla.merkle.westphall@ufsc.br*

ASSISTANT COORDINATOR: Caciano dos Santos Machado (CPD – UFRGS), *caciano@cpd.ufrgs.br*

TEAM: Carla Merkle Westphall, Caciano dos Santos Machado, Cristian Alves dos Santos, Eduardo Freitas Hoffmann

On-chain financial technology **with compliance for regulated institutions**

WHITE-LABEL SOLUTION FOR TRADING TOKENIZED ASSETS

Decentralized financial technology has opened new possibilities for asset negotiation and management, with programmability and verifiable settlement. However, it still faces challenges in regulated markets. Centralized exchanges remain dependent on custody, internal reconciliation, and centralized controls, while on-chain venues, open by design, do not yet fully meet the compliance requirements of financial institutions and Virtual Asset Service Providers (VASPs). This gap is where Levery positions itself.

As a white-label DEX stack focused on compliance, the platform enables institutions to create and operate compliant trading environments for tokenized assets. The solution abstracts the complexity of connection and authorization of on-chain transactions: clients can create their wallets within the institution's environment, with seamless onboarding, without relying on external wallet extensions. At the same time, the institution retains full control over credential management, usage policies, and access recovery without compromising user privacy. KYC, KYB, AML policies, eligibility rules, and risk limits are enforced through smart contracts audited by Levery before any liquidity operations take place. Additionally, the platform provides an administrative console, asset management policies, monitoring tools, API integrations, and oracles for rate adjustments. The result is an architecture designed to enhance institutional governance, reduce complexity for end users, and bring DeFi closer to the requirements of regulated financial markets. •

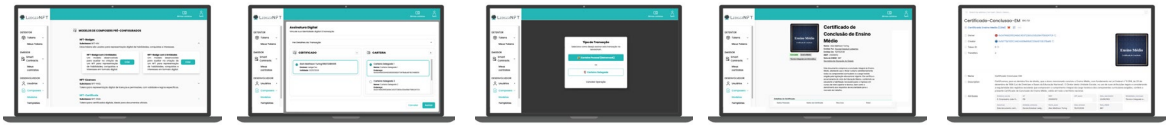
LEVERY COMBINES ON-CHAIN SETTLEMENT, COMPLIANCE, AND INSTITUTIONAL GOVERNANCE

TECHNICAL ***INFORMATION***

GENERAL COORDINATOR:
Cristiano Policarpo (Wireshape), *cristiano@wireshape.com*

ASSISTANT COORDINATOR:
Ingrid Gomes (Wireshape), *ingrid@wireshape.com*

QR CODE



LedgerNFT: a platform for modeling, issuance, and control of predictive lifecycle NFTs

TOKENIZED MANAGEMENT OF RELEVANT DIGITAL DOCUMENTS (RDD)

LedgerTec's patented Predictive Lifecycle (NFT-PC) NFT technology, combined with its low-code/no-code platform for modeling, issuance, and control of smart contracts and tokens, redefines the management of digital assets, particularly those associated with Relevant Digital Documents (RDD). The approach transforms NFTs from simple collectibles into structured instruments for governance and compliance. Unlike conventional NFTs, NFT-PC establishes predefined rules regarding who can interact with a given token, at what moment, and which attributes may be modified, ensuring a predefined, finite, and auditable workflow. This model enables multi-institutional governance, allowing multiple entities (issuers and controllers) to collaboratively manage the lifecycle of digital assets. Each token represents a single digital asset, maintaining a unique digital instance from issuance through delivery to the final recipient. Additionally, a digital anchor ensures that preservation-related state changes generating new versions of the asset do not compromise the integrity of previous views held by stakeholders and recipients. The project involves modeling pilot applications based on NFT-PC using the LedgerNFT platform, exploring how NFTs can incorporate logic, temporality, and data throughout their lifecycle in real-world scenarios. The goal is to position NFTs as complementary system components to support traceability, cooperation, and integration across data and digital assets. •

TECHNICAL ***INFORMATION***

GENERAL COORDINATOR:
Caio Souza Florentino (Ledgertec), *caio@ledgertec.com.br*

TEAM:
Caio Souza, Rodolfo Costa, Sebastião Mateus Marques, João Heitor Lopes, Lucas Barbotin, Rostand Costa

QR CODE

LedgerNFT

LEDGER TEC

TOKENIZED MANAGEMENT OF DIGITAL ASSETS GOVERNED BY FINITE MULTI-INSTITUTIONAL WORKFLOWS

Blockchain for analytical governance **in supply chains**

INFRASTRUCTURE FOR VALIDATION AND TRACEABILITY OF RAPID TESTS

The reliability of analytical data is essential in supply chains subject to strict regulation, such as agriculture, environmental monitoring, and international trade. In these contexts, laboratory methods considered gold standards continue to serve as references for certifications and audits. However, their large-scale application is often limited by costs, response time, and operational complexity. To expand analytical monitoring capabilities throughout production processes, Sollytech developed a blockchain-based digital infrastructure focused on traceability and governance of analytical data, within the scope of the Ilíada Program. The solution integrates three main components: a permissioned blockchain network based on Hyperledger Fabric, functioning as an immutable registry of analytical evidence; a machine learning module responsible for automated evaluation of assay tests; and an integration layer that connects analytical devices, users, and distributed infrastructure. Unlike traditional blockchain applications focused solely on data storage, this architecture incorporates analytical logic into transactional workflows through smart contracts capable of executing inferences from models trained off-chain. As a result, measurements performed in the field generate verifiable and auditable evidence in real time, increasing transparency and strengthening quality control processes across supply chains. •

SØLLYTCH

BLOCKCHAIN ENABLING ANALYTICAL MEASUREMENTS TO BECOME AUDITABLE EVIDENCE IN SUPPLY CHAINS

TECHNICAL ***INFORMATION***

GENERAL COORDINATOR:
Mônica Santana Vianna (Sollytch – Soluções Analíticas Inteligentes), *monicaviann@gmail.com*

TEAM:
Mônica Vianna, Wilson Melo Júnior, Walter Spolidoro, Kledisom Oliveira, Rebeca Cruz, Carlos Oliveira, Eduardo Martins

PARTNER ***INSTITUTIONS***

Sollytech and INMETRO (Brazil's National Institute of Metrology, Quality, and Technology)

QR CODE

Acredita Working Group: verifiable credentials for Digital Identity and Access

APPLICATION OF THE DECENTRALIZED DIGITAL IDENTITY MODEL

Today, most information systems rely on centralized identity management models or "identity silos", where users' personal data is stored by institutions acting as identity providers. Even when consent exists, users have limited control over their own information. To address this gap, the Decentralized Digital Identity (DDI) model shifts control back to the user, enabling individuals to manage their own data and decide what to share and with whom. Through mechanisms such as zero-knowledge proofs and selective disclosure, it becomes possible to perform transactions by revealing only the strictly necessary information. Within this context, the project developed Proofs of Concept (PoCs) to validate the use of Verifiable Credentials (VCs) as an authentication factor for users. Two main approaches were explored:

1. Hyperledger Indy-based solution built on a verifiable data infrastructure, leveraging the technological maturity of previous initiatives within the Ilíada project.

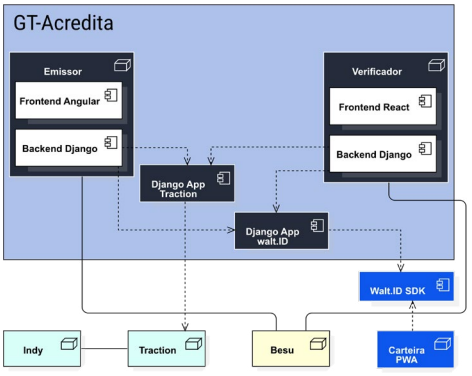
2. walt.id-based solution developed using the walt.id framework, a well-documented and consolidated tool, aiming to establish a reference model for developers seeking to implement DID in real-world applications.

Additionally, the project included a survey of open-source digital wallets, identifying solutions with the best usability and alignment with the technological choices adopted. •

TECHNICAL ***INFORMATION***

GENERAL/ ACADEMIC COORDINATOR:
Emerson Ribeiro de Mello (IFSC), *mello@ifsc.edu.br*

TEAM:
João Vitor (UFRGS), Kauan Freitas (IFSC), Marcos Wagner (IFSC), Rodrigo Lira (IFPE)



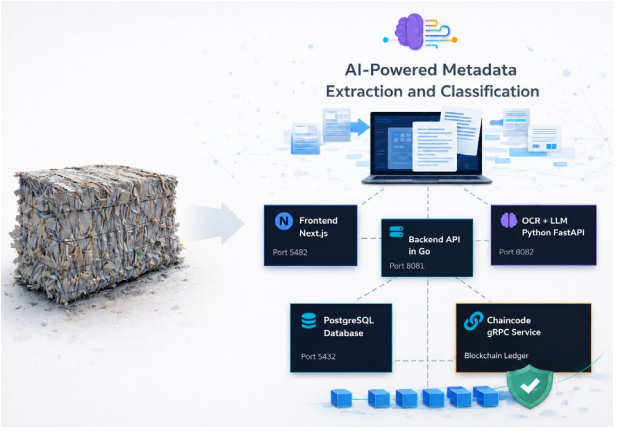
DEVELOPMENT OF ISSUER AND VERIFIER APPLICATIONS FOR VERIFIABLE CREDENTIALS

From paper to digital: AI and blockchain in the management of academic collections

INTELLIGENT AUTOMATION OF DOCUMENT DIGITIZATION IN HIGHER EDUCATION INSTITUTIONS

Brazilian higher education institutions have accumulated, over decades, large volumes of physical academic documents, such as student records, administrative files, and other institutional materials. The digitization and organization of these collections represent a significant challenge for universities and research centers, both due to operational complexity and the need to ensure integrity and retrieval of information. Within this context, the DAIESEB project, developed under the Ilíada project, proposes a technological solution that leverages Artificial Intelligence, computer vision, and blockchain to support the digitization and organization of academic archives. The platform enables the processing of digitized documents, including automated text extraction using OCR techniques and metadata structuring to facilitate organization and retrieval of academic information. As an additional security layer, cryptographic evidence of processed documents is recorded on a Hyperledger Fabric-based blockchain network, ensuring integrity and traceability over time. The solution was developed using a microservices-based architecture, enabling scalability and integration with existing academic systems. In this way, the initiative contributes to advancing digital transformation in Brazilian higher education, aligning with national initiatives such as the Digital Diploma and the Student Journey. •

AI AND BLOCKCHAIN APPLIED TO THE PRESERVATION AND MANAGEMENT OF ACADEMIC DOCUMENTS



TECHNICAL ***INFORMATION***

GENERAL COORDINATOR:
Rafael de Oliveira Durá Escrich (Certisecure Serviços Digitais Ltda.), *rafael.escrich@gmail.com*

ASSISTANT COORDINATOR:
Kamila Estevam (Certisecure Serviços Digitais Ltda), *kamilaestevam@gmail.com*

TEAM:
Rafael de Oliveira Durá Escrich, Kamila Estevam, Jean Martina, Lucas Palma

QR CODE

CYBER SECURITY

TRAINING, INNOVATION AND COLLABORATION TO STRENGTHEN CYBERSECURITY IN THE COUNTRY

Hackers do Bem

TRAINING PROFESSIONALS AND DEVELOPING CYBERSECURITY SOLUTIONS

The *Hackers do Bem* program aims to train cybersecurity professionals and support the development of innovative solutions to strengthen the national cybersecurity ecosystem.

The program is structured in a progressive track that combines theoretical classes and hands-on activities, enabling students to apply the knowledge acquired in a real-world environment. In addition to training, the program promotes events such as Hackathons and *Capture The Flag (CTF)* competitions, which bring together technical challenges and collaborative activities focused on knowledge creation and sharing.

Within the R&D track, the program fosters projects focused on developing new cybersecurity tools and solutions. These initiatives are organized into 12 Working Groups across two cycles, involving more than 80 fellows in applied research activities, resulting in the training of qualified professionals to meet the growing demand for cybersecurity expertise.

In this edition, the program presents results from 5 Working Groups in the second R&D cycle. Complementing these actions, the program also advances the development of a national cybersecurity hub, connecting students, researchers, companies, and public institutions, promoting cooperation opportunities and strengthening the country's cybersecurity capabilities.

By integrating training, applied research, and institutional collaboration, Hackers do Bem contributes to reducing the shortage of specialists and strengthening cybersecurity in Brazil. •

TECHNICAL ***INFORMATION***

GENERAL/ ACADEMIC COORDINATOR:
Iara Machado (RNP), *iara.machado@rnp.br*

ASSISTANT COORDINATOR:
Alessandra Poubel (RNP), *alessandra.poubel@rnp.br*

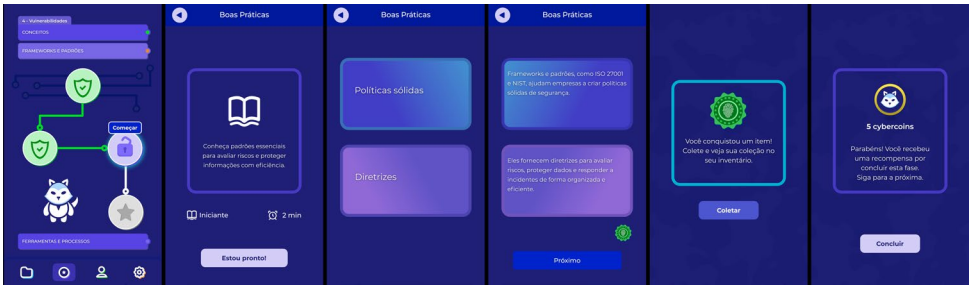
TEAM:
Leandro Guimarães, Emilio Nakamura, Michelle Wangham, Lisandro Granville, Stela Toti, Luciana F., Rômulo P., Yve M., Renato D., Cristian G.

QR CODE

Videobot: when learning cybersecurity becomes an interactive experience

MULTIMEDIA APPLICATIONS AND AI CAN TRANSFORM LEARNING

In a context where technology education evolves rapidly, student engagement does not always keep pace, making new teaching approaches essential. In this scenario, Videobot emerges as an approach that combines interactive multimedia applications, digital storytelling, and data analysis to support cybersecurity education. The initiative integrates the Hackers do Bem Program and is based on a simple idea: turning small moments of everyday life into learning opportunities. Instead of long sessions of expository content, students interact with short, structured episodes in which their decisions influence the unfolding of the narrative.Unlike traditional video-based lessons, where students passively consume content, Videobot uses interactive multimedia applications that respond to user choices. Each decision generates feedback within the narrative itself, allowing students to visualize consequences and learn through experimentation. Throughout the experience, the system captures interaction data—such as decision time, navigation paths, and response patterns—which can be analyzed to better understand learning behavior. This infrastructure enables the use of artificial intelligence for content recommendation, doubt clarification, and the adaptation of learning paths, contributing to a new generation of digital learning tools. •



IN VIDEOBOT, EACH CHOICE SHAPES THE NARRATIVE AND HELPS PERSONALIZE LEARNING

TECHNICAL *INFORMATION*

GENERAL/ ACADEMIC COORDINATOR:
Danielle Rousy Dias Ricarte (Universidade Federal da Paraíba - UFPB / LAVID), *danielle@lavid.ufpb.br*

ASSISTANT COORDINATOR:
Raoni Kulesza (Universidade Federal da Paraíba - UFPB / LAVID), *raoni@lavid.ufpb.br*

TEAM:
Barbara Cavalcante, Clarrissa Santos, Gustavo Campos, Herick Freitas, Matheus Honório, Pedro Alves, Pedro Silveira, Raissa Maiara

PARTNER *INSTITUTIONS*

Laboratory of Digital Video Applications (LAVID) / Workverse

QR CODE

We Got Hacked!
an educational game on cyber incident response

A GAME THAT SUPPORTS DECISION-MAKING

We Got Hacked! is a simulation game inspired by the day-to-day operations of a Security Operations Center (SOC), designed to teach incident response processes and strengthen decision-making skills. The project combines engaging gameplay with realistic cybersecurity incident scenarios. It centers on a conflict between an oil company and a hacktivist group. The player assumes different roles within the incident response team of a Managed Security Service Provider contracted to monitor the company's assets. The game is structured into three phases of increasing complexity, each representing a distinct cyber incident. In the first phase, the player must handle a phishing attack on the oil company's website. To resolve the incident, the player must make decisions guided by a playbook. The second phase simulates a ransomware attack triggered by a phishing breach within the company. In the final phase, the player must respond to a data breach caused by the exfiltration of confidential data by the hacktivist group. We Got Hacked! is an innovative cybersecurity education project tailored to the Brazilian context; therefore, the game was developed in Portuguese. •

THE GAME'S GOAL IS TO SUPPORT THE TRAINING OF PROFESSIONALS TO WORK IN A SOC

TECHNICAL ***INFORMATION***

GENERAL/ ACADEMIC COORDINATOR:
Luciano Ignaczak (Unisinos), *lignaczak@unisinos.br*

TEAM:
Bernardo Klein, Frank Veja, Igor Flores, Jairo Augusto de Campos Alff, Mauricio Bammann Gehling, Rodrigo Steigleder, Tiago Umberto Gazzola

PARTNER ***INSITUTIONS***

Universidade do Vale do Rio dos Sinos (UNISINOS), Atomic Rocket Solutions, ServiceIT Security, DropReal, CAIS RNP

QR CODE

ANONYMIZED REAL INCIDENTS BECOME PRACTICAL TRAINING WITH AI AND HUMAN VALIDATION

Learn From Incidents: ireal incidents become training for cyber defense

A SOLUTION INTEGRATING HANDS-ON TRAINING AND OPERATIONAL SUPPORT

Learning to respond to security incidents goes beyond theory. It requires contact with real-world situations, decision-making under pressure, and an understanding of the operational flows used by frontline professionals. Learn From Incidentes (LFI) Working Group (WG) was created precisely to bridge training and operational practice by transforming anonymized real incidents into learning experiences and support for incident response. Developed within the Hackers do Bem Program, the project integrates four fronts: anonymization of sensitive data, automated classification of incidents using AI, human validation by trainees and analysts, and a gamified platform focused on skills development. The result is a solution that helps train new professionals while also making the analysis and standardization of security tickets in PoPs and CSIRTs more agile. In 2025, LFI WG delivered a functional MVP, validated with real incidents, and achieved significant results in research and innovation, including papers accepted at national and international scientific conferences. The next step is to expand the incident base, refine the platform experience, and advance the consolidation of the solution as a reference for training and support in incident response. •

TECHNICAL ***INFORMATION***

GENERAL/ ACADEMIC COORDINATOR:
Rodrigo Sanches Miani (UFU), *miani@ufu.br*

TEAM:
Silvio Ereno Quincozes, Diego Luis Kreutz, Leandro Bertholdo

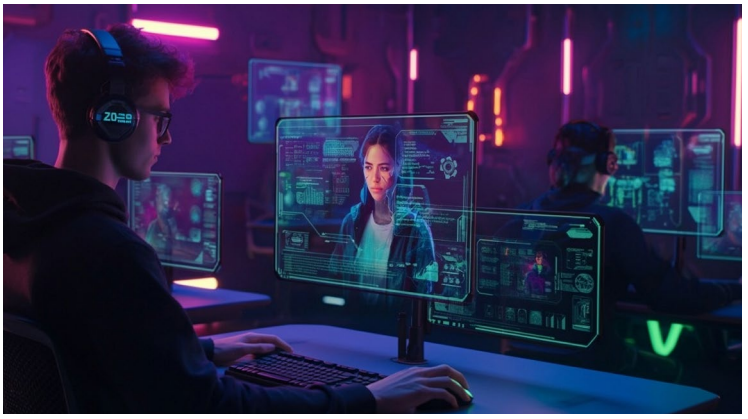
PARTNER ***INSITUTIONS***

UFU, UNIPAMPA, UFRGS

QR CODE

Invada o **CASTELO**

TEACHING ATTACK AND DEFENSE IN SYSTEMS AND NETWORKS



A COMPLETE AND FLEXIBLE PLATFORM FOR CYBERSECURITY COMPETITIONS AND TRAINING

The CASTLE platform was designed to provide efficiency in hosting and simultaneously managing multiple challenges, tracks, and events. To achieve this, it uses virtualization strategies, dynamically adjusting resources according to user profiles and demand, with options for creating attack and defense scenarios.

Although this model requires greater computational resources, it offers a higher level of isolation in CTF environments, which is essential for certain types of challenges. Given the current cybersecurity landscape, an important challenge arises: ensuring security in light of the constant evolution of emerging technologies and the high value of operations and stored data.

Addressing this challenge requires training specialized cybersecurity professionals capable of identifying vulnerabilities and developing effective countermeasures. In this context, the CASTLE platform serves as a tool that integrates didactic cybersecurity challenges and practices, including activities such as red, blue, and purple team exercises.

The platform includes training activities and competitions tailored to the needs of individuals, groups, and institutions. Among its distinguishing features are a gamification system based on knowledge levels and a recommendation system for activities, competitions, and adversaries aligned with these levels. •

TECHNICAL *INFORMATION*

GENERAL/ ACADEMIC COORDINATOR:
André Ricardo Abed Grégio (Universidade Federal do Paraná - UFPR), *gregio@ufpr.br*

ASSISTANT COORDINATOR:
Vinicius Fülber Garcia (Universidade Federal do Paraná - UFPR), *viniciusfulber@ufpr.br*

TEAM:
André Grégio, Vinicius Garcia, Nadia Lobkov, Jorge Correia, João Andreotti, Claudio Torres Jr., Fernando Kiotheka, Matheus Herbele

QR CODE

A New Frontier in Cyber Threat Detection: **RNP Vulnerabilities**

RAPID VALIDATION OF VULNERABILITIES IN THE RNP SYSTEM

The growing number of vulnerabilities in networks and applications demand agile and automated solutions. SITV Working Group, developed by UFRN during the 2nd Hackathon RNP, was created to strengthen the digital security of the RNP System through a web platform focused on the identification and mitigation of vulnerabilities.

The tool enables managers and analysts at Points of Presence (PoPs) to validate vulnerabilities reported by SGIS within minutes, without requiring deep technical expertise. The process includes federated login via CAFe, vulnerability selection, automated validation, and the generation of professional reports with specific remediation recommendations.

With API support for integration with other systems, SITV WG promotes continuous validation and interoperability. Results from the Proof of Concept with PoPs in Bahia, Pernambuco, and Paraná demonstrated improvements in time efficiency, automation, and compliance.

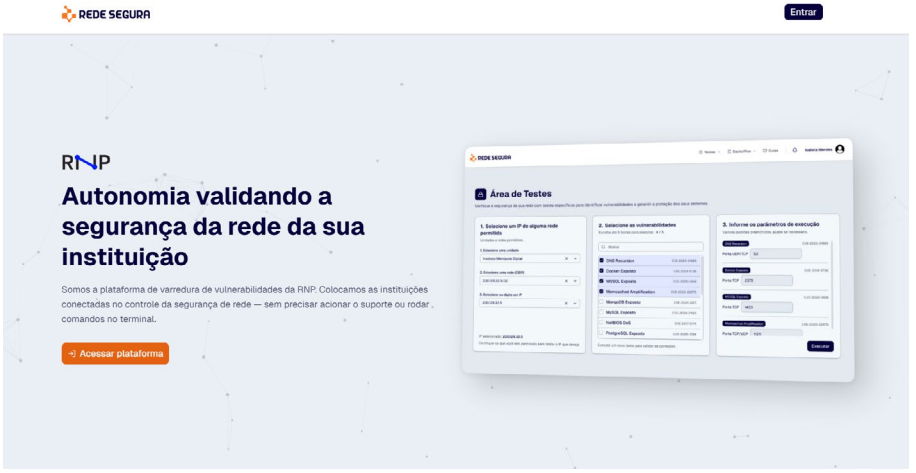
The project is consolidating itself as a significant step toward simpler, more adaptable, and efficient security management across the RNP System. •

TECHNICAL ***INFORMATION***

GENERAL/ ACADEMIC COORDINATOR:
Rildo Antonio de Souza (RNP), *rildo.souza@rnp.br*

TEAM:
Matheus Vidal, Paula Marinho, Isabela Gomes

QR CODE



SITV WG VALIDATES SGIS NOTIFICATIONS IN MINUTES FOR RNP POPS VIA WEB

Technical Committee **on Cybersecurity**

CYBERSECURITY DATA AVAILABLE TO THE COMMUNITY

The Call for Proposals under the Cybersecurity Technical Committee (CT-Cibersegurança) aimed to develop an infrastructure for collecting, anonymizing, and publishing cybersecurity datasets.

Vulnerability and incident reports collected by RNP were made available by the Security Incident Response Center (CAIS). To anonymize these reports, four projects were developed by researchers from UFCG, UFF, UFRJ, and Unipampa.

The projects focused on developing an open-source workflow with tools and methods to transform and analyze the usefulness of anonymized output data. The approach includes an automated anonymization method that applies k-anonymity through suppression of structured attributes and regression with Bayesian optimization.

It also incorporates a semantic anonymization algorithm using Transformer-based language models for data labeling, as well as a pseudonymization method based on HMAC-SHA256 to generate strong and reversible pseudonyms.

The next step is to make the results of these projects and the anonymized cybersecurity datasets available to the community, addressing a demand raised by Cybersecurity Technical Committee members to support scientific research. •

TECHNICAL ***INFORMATION***

GENERAL/ ACADEMIC COORDINATOR:
Igor Moraes (UFF),
igor@ic.uff.br

ASSISTANT COORDINATOR:
Ian Bastos (UERJ),
ian.bastos@eng.uerj.br

TEAM:
Secretary:
Reinaldo Gomes

QR CODE

TECHNICAL FORESIGHT PROJECTS DEVELOPED SOLUTIONS FOR DATA ANONYMIZATION

RD&I *FOR ADVANCED SERVICES*

MaisAção: Gamifying Curricular Integration of Extension Activities

AN AI-BASED PLATFORM

Curricular integration of extension activities is a central strategy for connecting teaching, research, and extension, promoting socially relevant education aligned with real-world demands. However, there is still a lack of technological tools that support its integrated implementation—especially regarding the systematic management of institutional evidence and student engagement—given the requirement that at least 10% of course workloads be dedicated to extension activities.

In this context, the MaisAção Working Group proposes a platform to organize curricular extension in an integrated way. The solution enables the academic community to register external demands directed to Higher Education Institutions (HEIs), which are then screened and forwarded to faculty members or stored in an opportunity database.

Based on these demands, professors create extension actions, open enrollment for students, record evidence, and assign strategies for engagement. The platform also provides APIs for integration with academic systems, dashboards for monitoring workload, and AI-based features to streamline registration processes, as well as a public module for disseminating results. The tool is currently being tested at UFRGS, UFCSPA, UENF, and UFES.

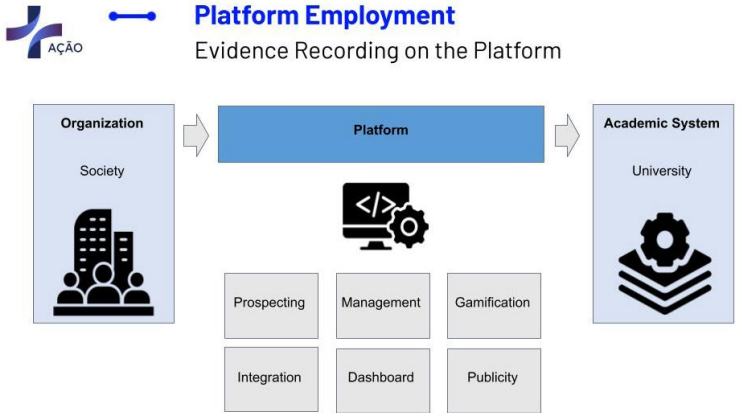
TECHNICAL ***INFORMATION***

GENERAL/ ACADEMIC COORDINATOR: Ricardo Tombesi Macedo (Universidade Federal de Santa Maria), *ricardotombesi@ufsm.br*

INNOVATION LEAD: Betania Vahl de Paula (Startup Performance Vegetal), *contato@performancevegetal.com.br*

TEAM: Arthur Guarizi de Godoy, Eliane Cristina Amoretti, Karina Lira Ohara, Leon Tassinari Julião, Marco André Babinski

QR CODE



A PLATFORM THAT ORGANIZES THE ENTIRE PROCESS OF CURRICULAR INTEGRATION OF EXTENSION ACTIVITIES

Towards CAFe 2.0: BAITA WG Proposes a New Federated Infrastructure

PROJECT MODERNIZES THE ACADEMIC FEDERATION

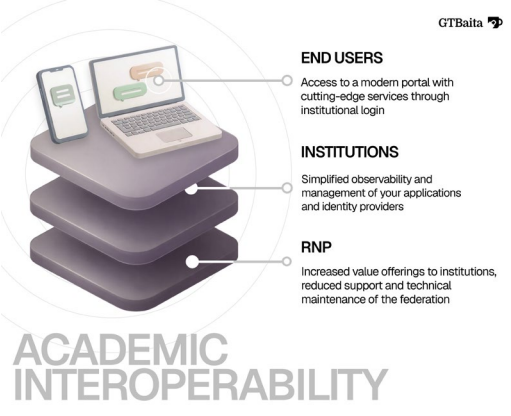
The Federated Academic Community (CAFe) connects more than 320 education and research institutions in Brazil, enabling students, professors, and researchers to use their institutional credentials to access digital services offered by different organizations.

Many end users are not aware that the availability of CAFe-enabled services and applications still occurs in a limited way. As a result, CAFe is often perceived merely as an access mechanism to RNP services, rather than as a broader environment for digital collaboration.

In this context, the Working Group on Academic Interoperability Framework (BAITA WG) proposes an evolution of the federation. The initiative seeks not only to modernize CAFe technologically, but also to reposition it as an ecosystem for academic interoperability, promoting integration and expanding the sharing of digital services and resources among institutions.

Among the key components of this framework are: a Federation Management System, which simplifies onboarding and the administration of identity and service providers; a User Portal, designed to integrate user services within their home institution and RNP into a single environment, using federated authentication, along with data collection for service metrics and observability; and a Web Application Firewall (WAF), which, in addition to its traditional role, also functions as a syntactic and semantic normalizer for user identity attributes. •

THE PROJECT PROPOSES A NEW ARCHITECTURE TO EXPAND THE ROLE OF CAFE IN ACADEMIC COLLABORATION



TECHNICAL *INFORMATION*

GENERAL/ ACADEMIC COORDINATOR: Frederico Schardong (Instituto Federal do Rio Grande do Sul), *frederico.schardong@rolante.ifrs.edu.br*

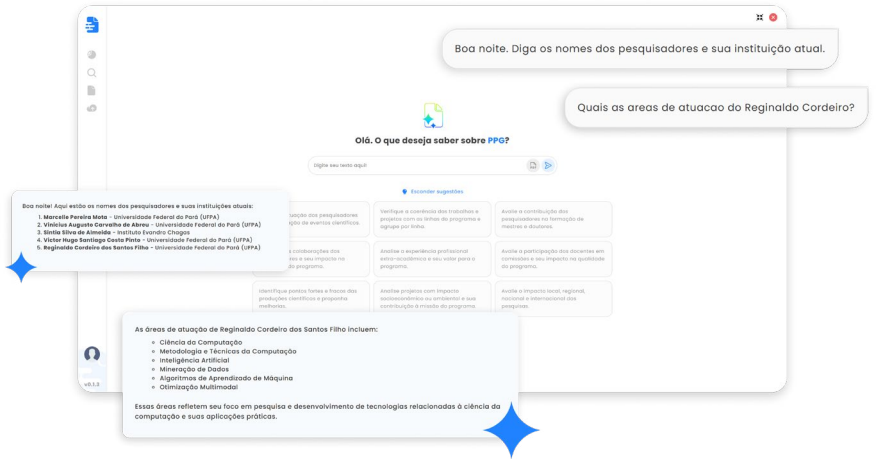
INNOVATION LEAD: Eduardo Perottoni (Universidade Federal de Santa Catarina), *edu.perottoni@gmail.com*

TEAM: Ricardo Custódio, Brendon V. Silva, Giulia Manno Lima, Alison De Rozado Batista, Leonardo M. dos Passos, Charlie E. Terra, Raissa M. Lima, Rayane M. Castilhos

PARTNER *INSTITUTIONS*

IFRS e UFSC

QR CODE



Intelligent Academic Management with the **AVIDA.AI Plataform**

INTEGRATED SCIENTIFIC DATA FOR STRATEGIC DECISION-MAKING

The AVIDA.AI platform supports course coordinators and graduate programs in making data-driven decisions based on consolidated information. By automatically integrating multiple national and international academic databases, the solution organizes, cross-references, and interprets scientific information in a strategic way.

Through automated analysis capabilities, natural language processing, and artificial intelligence, AVIDA enables continuous monitoring of research output indicators, evaluation of national and international impact, tracking of funding opportunities, mapping of collaborations among researchers, and identification of strategic opportunities.

The platform also supports the continuous improvement of graduate programs. Coordinators move beyond simply monitoring evaluations and begin conducting ongoing self-assessments, anticipating risks and strengthening program planning.

Its conversational interface functions as a management copilot, answering strategic questions in natural language and transforming dispersed data into objective insights about the real situation of the program going beyond traditional reports.

AVIDA promotes evidence-based governance and continuous improvement of institutional performance. •

TURN ACADEMIC DATA INTO MANAGEMENT INTELLIGENCE

TECHNICAL *INFORMATION*

GENERAL/ ACADEMIC COORDINATOR:
Reginaldo Santos (Universidade Federal do Pará), *regicsf@ufpa.br*

INNOVATION LEAD:
Sintia Silva de Almeida (Universidade Federal do Pará), *sintiaalmeida@gmail.com*

TEAM:
Vinícius Abreu, Marcelle Mota, Victor Pinto, José Perdigão, Thiago Correa, Cristiano Monteiro, Helder Matos, Atílio Azevedo

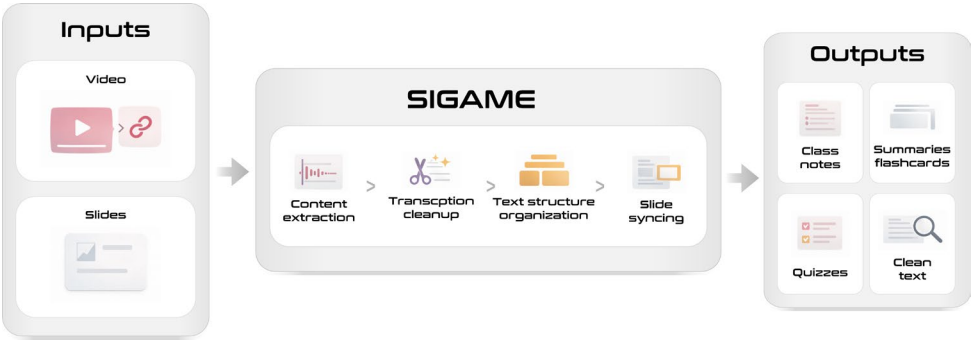
STARTUP *PARTNER*

Katu Data Visualization

QR CODE

SIGAME: From Video to Study Material in Minutes

AI TO TRANSFORM RECORDED LECTURES INTO SUPPLEMENTAL CONTENT



Recorded lectures, webinars, and training sessions are multiplying in educational institutions, but the content remains largely confined to hours of video. Reviewing, locating a specific section, and transforming the recording into study or reference material often requires time and effort. SIGAME (Intelligent System for Automatic Generation of Educational Materials) solves this bottleneck: from a video uploaded as a file or link, the solution produces materials ready for study and research. When the user attaches a PDF of slides, the images are incorporated throughout the text as a reference, facilitating reading, navigation, and comprehension.

With SIGAME, the same content can become detailed, organized lecture notes, objective summaries, flashcards, and exercise lists, as well as a processed text version, ideal for searching and knowledge bases. In initial assessments, the preventative solution reduces the time spent on reviewing and organizing material by approximately 60%, compared to the common transcription workflow and processing with generic AI.

SIGAME is developed within the scope of RNP's Advanced Services R&D Program, aimed at the teaching and research community, in partnership with CRIAR, from CIn-UFPE.

FROM VIDEO TO SUPPLEMENTAL MATERIAL: FAITHFUL TO THE ORIGINAL CONTENT, WITH INTEGRATED SLIDES

TECHNICAL *INFORMATION*

GENERAL/ ACADEMIC COORDINATOR:
Tsang Ing Ren (CIn-UFPE), *tir@cin.ufpe.br*

INNOVATION LEAD:
Paulo Borba (CIn-UFPE), *phmb@cin.ufpe.br*

TEAM:
Érico Medeiros, João Oliveira, Kauã Lima, Lígia Padilha, Lucas Goncalves, Mateus Baltazar, Rafael Barros

PARTNER *INSTITUTIONS*

CRIAR - Center for Innovation in Robotics and Responsible Artificial Intelligence

QR CODE

IoTEdu: Secure Connectivity with Artificial Intelligence for Academic IoT

PLATFORM AUTOMATES DEVICE ONBOARDING AND RISK MONITORING IN IOT

In many Brazilian universities, it can still take two to six business days to enable an IoT device on the network. In some cases, the process raises security concerns due to the lack of control and visibility over connected devices.

IoTEdu addresses this challenge by providing a connectivity platform designed for academic IoT environments. Developed within the IoTEdu Working Group at RNP, coordinated by UNIPAMPA in partnership with UFRGS, UFU, and UFF, the project delivers a specialized solution for managing connected devices in teaching and research contexts.

The platform enables rapid onboarding of IoT devices through federated authentication, centralized inventory management, and the application of access policies tailored to academic environments.

Within minutes, faculty and researchers can autonomously register devices, while IT teams gain access to a unified dashboard to monitor connectivity, compliance, and device behavior.

At its core, the platform is based on a multilayer security architecture integrating intrusion detection systems (IDS) with machine learning techniques, capable of identifying known attacks and detecting anomalous behavior on the network.

Pilot deployments are planned for 2026 at UNIPAMPA, UFRGS, and UFU, with potential expansion to university hospitals, Industry 4.0 environments, and the agribusiness sector. •

IOT DEVICES REGISTERED IN SECONDS AND MONITORED BY ARTIFICIAL INTELLIGENCE

TECHNICAL *INFORMATION*

GENERAL/ ACADEMIC COORDINATOR:
Diego Kreutz (Unipampa), *diegokreutz@unipampa.edu.br*

INNOVATION LEAD:
Vagner Quincozes (UFF), *vequincozes@id.uff.br*

TEAM:
Leandro Bertholdo, Rodrigo Mansilha, Rodrigo Miani, Silvio Quincozes, Angelo N., Anna R., Douglas F., Emanuel C., Joner A., Leonardo B., Matheus C.

PARTNER *INSTITUTIONS*

UNIPAMPA, UFRGS, UFU, UFF

QR CODE

LLMestre Working Group

PROVISION AND CREATION OF ACADEMIC CONTENT USING AI AGENTS

University professors face a significant workload when designing new courses, developing content, and preparing teaching materials. This workload often reduces the ability to update courses frequently and limits the diversity of disciplines offered.

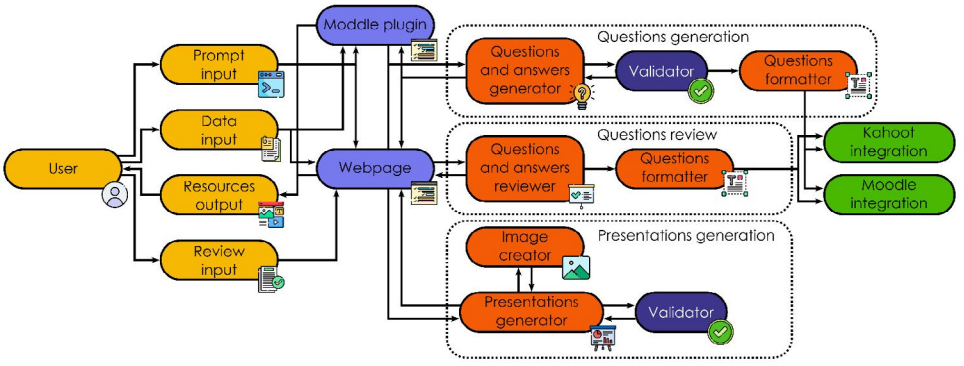
To address this challenge, the LLMestre Working Group develops a platform to automate the creation of educational content using specialized AI agents integrated with Large Language Models (LLMs).

The platform implements an agent-based framework using LangFlow, where different AI agents perform specific tasks across the content creation workflow.

Through a web interface, users can access the platform and optionally integrate it with Moodle via a plugin. For creating presentations and quizzes, users enter a structured prompt and upload supporting documents as input data.

Outputs are generated as structured teaching materials. One of the platform's key design principles is to ensure that content is generated strictly based on the materials provided by the instructor, reducing the risk of LLM hallucinations.

After generating a quiz, users can perform a review step through a dedicated revision input. The agents then refine the content based on user feedback, ensuring alignment with instructional objectives. •



THE LLMESTRE WORKING GROUP DEVELOPS A PLATFORM TO AUTOMATE THE CREATION OF EDUCATIONAL CONTENT

TECHNICAL *INFORMATION*

GENERAL/ ACADEMIC COORDINATOR:
Rodrigo de Souza Couto (UFRJ), *rodrigo@gta.ufrj.br*

INNOVATION LEAD:
Leonardo Picciani (Black Bear Bytes), *leo@blackbearbytes.com*

TEAM:
Felipe Táparo, Fernando Silva, Guilherme Silva, João Sobrinho, Lucas Souza, Luís Costa, Maria Sales, Miguel Campista, Pedro Cruz, Pedro Rubinstein

QR CODE

Sokrates.AI

A SOCRATIC KNOWLEDGE PLATFORM

Sokrates.AI is an intelligent mentor for higher education, based on Generative Artificial Intelligence and the Socratic Method, designed to promote active learning, critical thinking, and intellectual autonomy.

Unlike traditional tutors, it does not simply provide answers; instead, it guides students through questions, reflections, and challenges that stimulate knowledge construction. The solution addresses real-world higher education challenges by offering personalized and engaging learning experiences, placing the student at the center of the teaching-learning process.

For institutions, the platform contributes to increased engagement and reduced dropout rates. Using proprietary LearningFlow technology, Sokrates.AI organizes knowledge construction through adaptive learning journeys based on Socratic dialogue.

A digital twin of the learner models competencies, knowledge gaps, and learning preferences, enabling personalized guidance. Inspired by Self-Determination Theory, the platform fosters autonomy, competence, and a sense of belonging.

Learning is reinforced through exercises, self-assessments, and challenges integrated into students' daily routines.

Technically, Sokrates.AI is built on an agent-based architecture, leveraging multiple intelligent agents, specialized services, and Large Language Models (LLMs). The platform transforms passive knowledge consumption into a continuous process of discovery and active knowledge construction. •

PERSONALIZED LEARNING AND AI-DRIVEN SOCRATIC MENTORSHIP TO TRANSFORM EDUCATION

TECHNICAL *INFORMATION*

GENERAL/ ACADEMIC COORDINATOR:
Geraldo Bonorino Xexéo (COPPE/ UFRJ), *xexeo@cos.ufrj.br*

INNOVATION LEAD:
Claudio Dipolitto (InoveLab: Inovação, Cultura e Desenvolvimento LTDA), *claudiodipolitto@gmail.com*

TEAM:
Claudia Susie Camargo Rodrigues, Débora de Oliveira Souza, Gabriele Iwashima, Luiz Felipe Cantanhede Cristino, Vitória Nazareth, Thomas Cardoso

QR CODE

27°

Workshop
RNP

openRAN BRASIL

OpenRAN@Brasil is an MCTI program that promotes open networks in Brazil through research, innovation, and capacity building in 5G and beyond. Coordinated by RNP and jointly executed by RNP, CPQD, Inatel, and Eldorado, the initiative expands national testing and infrastructure capabilities, fostering applications in industry, agriculture, smart cities, and education. The program is part of the Priority Program for Advanced Internet Informatics (PPI) and is funded under Law No. 8,248 of October 23, 1991 (Brazilian Informatics Law).

Learn how your institution can use the program's testbed:

https://openranbrasil.org.br/

EXECUTION

RNP cpqd ELDORADO INSPIRAÇÃO PELO NOVO Inatel

COORDINATION

RNP

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO

BRAZILIAN GOVERNMENT BRASIL STANDING WITH THE BRAZILIAN PEOPLE

Project supported by the Ministry of Science, Technology and Innovation, funded under Law No. 8,248 of October 23, 1991, in accordance with regulations from the Secretariat for Entrepreneurship and Innovation.