De CLARA

Cooperación Latino Americana de Redes Avanzadas

BULLETIN
62
AUGUST
2026

eduLACSeg: The defense force of Latin America's largest academic cybersecurity ecosystem

Colombia: RENATA drives historic connectivity in communities

Helsinki Declaration

RedCLARA
Cooperación Latino Americana de Redes Avanzadas

Contents

Content and general editing: María José López Pourailly

Design: Marcela González Garfias

Translations into English and Portuguese carried out using DeepL.

Juan Pablo Carvallo Vega
Executive Director of CEDIA
Board Member of RedCLARA

Cooperating to compete: the strength of Latin American NRENs

A few years ago, at CEDIA, we asked ourselves a question that transformed our understanding of internationalisation: what would happen if, alongside lecturers, researchers and students, we also involved vice-chancellors, pro-vice-chancellors and deans in experiences capable of enriching the strategic vision with which our universities are led?

From that reflection came the first immersion trip for vice-chancellors. It was not conceived as a ceremonial mission, but as an opportunity to observe other models, compare experiences and return with new questions. Today, after six international immersion trips – the most recent in China – we can confirm that their true value lies not only in what is learnt during the trip, but in what happens afterwards: when a conversation leads to a decision, when an international model is adapted to the local context, and when an idea inspires institutional transformation.

But these experiences have also led us to a broader conclusion. One of the main challenges facing Latin America and the Caribbean is not a lack of talent or valuable initiatives, but the fragmentation of our capabilities. In science and technology, acting in isolation is becoming increasingly costly: efforts are duplicated, solutions are developed that do not interact with one another, and the scale required to make an impact is lost.

That is why National Research and Education Networks (NRENs) play a strategic role. Their mission goes far beyond connecting institutions through advanced infrastructure. An NREN connects communities, builds trust, identifies common needs and creates the conditions for universities and research centres to collaborate on a sustained basis. And when Latin American NRENs are linked through RedCLARA, national capabilities can become regional capabilities.

This opens up an extraordinary opportunity: to develop common platforms, services and tools that function as genuine digital public goods for higher education and science. We can share and co-develop solutions for cybersecurity, federated identity, open science, data management, artificial intelligence, remote laboratories and scientific collaboration. And on that basis, we can promote consortia and research and innovation projects that bring together critical mass, talent, data and infrastructure from various countries. It is not a question of all networks doing the same thing, but rather of each contributing what it does best, and ensuring that what is developed in one country can be reused, adapted and improved by others.

This model reduces costs and duplication, accelerates learning, raises standards and extends the benefits of joint developments to the entire regional academic ecosystem. It also strengthens the technological sovereignty of Latin America and the Caribbean, an increasingly urgent issue in a world where artificial intelligence and data governance are redefining who makes the decisions and who is dependent. Sovereignty does not mean isolating ourselves or producing everything ourselves, but rather having the knowledge, talent, infrastructure and agreements to decide which technologies to adopt, how to adapt them, how to govern and share our data, and which solutions to develop in line with the region's priorities. In this way, Latin America and the Caribbean participate not only as users, but also as creators, operators and technology partners, with their own voice and agenda.

Ongoing initiatives already demonstrate that this vision is possible. eduLACSeg, the cybersecurity group of the region's NRENs, shares threat intelligence, methodologies and training, and has built a community capable of responding confidently to incidents. The Latin American and Caribbean University Telemedicine Network (RUTE-ALC), promoted by the NRENs with support from RedCLARA, applies this same approach to healthcare through scientific and educational cooperation and joint telehealth projects. And SCALAC, the Advanced Computing System for Latin America and the Caribbean, extends this approach to supercomputing: it brings together centres, academic networks and scientific communities to share infrastructure, train talent and facilitate data-intensive research.

These three examples demonstrate how distributed capabilities can be transformed into regional platforms serving science and society.

In this context, the rectors' immersion programmes take on a deeper meaning. They seek to strengthen leadership capable of transforming learning into shared agendas – an effect that is multiplied when vice-chancellors, pro-vice-chancellors and deans link that vision to the day-to-day work of lecturers, researchers and students. Upon returning, the question is no longer simply 'what can we incorporate into our university?', but rather 'what can we develop with other institutions, what infrastructure can we share, and what regional problem can we solve together?'. In this way, internationalisation ceases to be mere observation and becomes co-creation.

This is, moreover, a more mature – and profoundly Latin American – way of understanding international cooperation. Not as unilateral aid, but as horizontal cooperation, in the finest tradition of South-South cooperation: sharing risks, investment, knowledge and results amongst peers. Partnerships with other regions will remain indispensable, but they will be more valuable if Latin America and the Caribbean approach them with their own agenda, coordinated capabilities and the ambition to participate as a scientific and technological partner, rather than merely as a user.

Our region's competitiveness will depend, to a large extent, on how quickly we manage to transform knowledge into solutions, connect talent, access high-level infrastructure and scale up innovations. In this context, collaboration is not the opposite of competition: it is, in fact, the very condition that enables us to compete more effectively.

The next step is to transform scattered projects into a sustained regional portfolio: mapping capabilities, agreeing on priorities, adopting open standards, sharing governance and funding, and measuring impact. At RedCLARA, trust amongst the NRENs translates into common agendas, shared projects and services designed with a regional scope. Each network's close connection to its national needs is thus combined with the diversity, scale and global reach of Latin American and Caribbean cooperation.

After six immersive visits and numerous initiatives with our sister networks, the lesson is clear: the region makes greater progress when universities, countries and NRENs turn their strengths into a shared agenda. When one network innovates, the others learn; when several co-develop, the region accelerates; and when RedCLARA coordinates this effort, science crosses borders and translates into development and well-being.

> **Cooperation does not mean giving up competition. It means deciding that Latin America and the Caribbean will compete as a region: with their own knowledge, shared infrastructure, technological sovereignty and science at the service of their people.**

Colombia: RENATA drives historic connectivity in communities north of the Magdalena River

For the first time, an underwater fibre-optic network has crossed the Ciénaga Grande de Santa Marta to connect stilt-house communities and strategic municipalities north of the Magdalena River, in an initiative led by Colombia's Ministry of Information and Communications Technologies and implemented by RENATA, the country's National Research and Education Network (NREN) and a member of RedCLARA.

María José López Pourailly

Launched during the first half of June (two years after the signing of the agreement that paved the way for its implementation), the initiative marks a milestone for connectivity in Colombia by deploying fibre-optic infrastructure in particularly complex geographical conditions, with the aim of bringing high-speed internet access to communities built on the water and to areas historically remote from major urban centres.

And when we say 'particularly complex', it is important to note that, in order to reach this highly isolated population in such rugged landscape, RENATA had to assess and implement infrastructure never before undertaken in Colombia. This is the first time an underwater fibre-optic cable has been laid in the country; the total length of this network comprises 62 km underwater and 342 km of terrestrial fibre-optic cable. Those 62 km represent a major milestone given their complexity and innovation, which is unprecedented in the country.

The project enabled the municipalities of Ciénaga, Pueblo Viejo, Sitionuevo and Remolino, as well as the stilt-house communities of Buenavista and Nueva Venecia, to be connected via a technological solution combining 62 kilometres of sub-marine fibre-optic cable and 342 kilometres of terrestrial fibre-optic cable.

Thanks to the infrastructure deployed by RENATA, 14,158 households now have internet connectivity: 8,477 in Ciénaga, 3,005 in Pueblo Viejo, 1,952 in Sitionuevo, 90 in Remolino and 634 in the stilt-house villages. Beyond internet access and its obvious benefits, the initiative opens up new possibilities for education, knowledge, digital services, inclusion and local development.

RENATA plays a strategic role in strengthening the country's digital infrastructure and in coordinating efforts that bring communities closer to the knowledge ecosystem. Its participation in this initiative—which not only focused on technological development but also involved supporting the community through training, fostering ownership and promoting the correct use of ICT—reaffirms the value of advanced academic networks as enablers of social transformation, cooperation and innovation.

For RedCLARA, this development represents a concrete example of how national research and education networks contribute to bridging the digital divide in Latin America, by promoting infrastructure that connects regions, expands opportunities and strengthens equitable access to education, science and technology.

Helsinki Declaration: A growing global alliance to support Earth Observation

Senior representatives of ASREN, GÉANT, RedCLARA, TEIN*CC, UbuntuNet Alliance and WACREN have signed the Helsinki Declaration on 10 June 2026 during TNC26 in Helsinki, Finland. Building on the foundations of the Katowice Declaration first signed in 2021, the renamed declaration marks a significant milestone: the joining of TEIN*CC as a new partner, bringing the Asia-Pacific region into a truly global coalition of Regional Research and Education Networks (RRENs) committed to advancing Earth Observation for the benefit of society.

The declaration has been renamed the Helsinki Declaration to reflect both this expansion and the significance of the Finnish capital as the location of signature at TNC26.

From Katowice to Helsinki

The journey began at the Internet Governance Forum in Katowice, Poland, in December 2021, when ASREN, GÉANT and RedCLARA joined forces to affirm their shared commitment to supporting the international Group on Earth Observations (GEO). The Katowice Declaration was formally signed at TNC22 in Trieste, Italy, in June 2022. A first expansion followed in June 2023, when UbuntuNet Alliance and WACREN joined, extending the coalition's reach into sub-Saharan Africa. Today, with the addition of TEIN*CC, the research and education network collaboration centre for the Asia-Pacific region, the partnership now connects research and education communities from the Arab states, Europe, Latin America, Africa and Asia-Pacific under a common vision.

Why Earth Observation matters

Addressing the UN Sustainable Development Goals, tackling climate change, and preparing for and responding to disasters all depend on data. Increasingly, this data is being centralised into vast datasets from a growing variety of sources, with volumes expanding exponentially as technology advances. Geospatial research, the investigation of earth science with a focus on specific locations, relies on robust communication layers and distribution systems to move that data efficiently across the globe.

The Helsinki Declaration recognises that RRENs are uniquely positioned to serve as the backbone of this data exchange, connecting researchers across borders and continents. It is their networks that

transport the observation data, analysis and education materials essential for addressing climate change.

The Declaration sets out a series of concrete commitments across several areas that are expected to have tangible societal impact:

- The partners commit to working towards a rapid and fluid exchange of GEO data across continents, addressing current technical challenges in synchronising platforms and continuing to upgrade infrastructure to meet the present-day requirements of research communities.
- The declaration emphasises the need to develop human capacity within the research and education community on Earth Observation topics, with a particular focus on increasing digital literacy, especially for women in the GEO ecosystem.
- Partners affirm that open access policies should be developed to ensure that GEO data can be accessed and used as widely as possible.

TEIN*CC is pleased to join the Helsinki Declaration in support of the global GEO community. Representing the Asi@Connect community across the Asia-Pacific region, we remain committed to strengthening trusted and inclusive digital connectivity for international research collaboration and Earth observation data exchange, and will continue working closely with our partners to advance these efforts”

– Presidente Jungsu Song, TEIN*CC–

• The partners commit to increased outreach and engagement with these communities, and to better understanding research priorities on each continent in order to identify areas for effective collaboration.

• The declaration also affirms that RRENs - and their NREN members - provide mechanisms enabling the realisation of many UN Sustainable Development Goals, and calls for partners to baseline their current contributions in this regard.

You can read the full Helsinki Declaration here.

The CEDIA Rectors’ Community undertook its sixth immersion trip

The delegation of rectors, as part of the immersive experience organised by Ecuador’s National Research and Education Network, visited 16 strategic locations within the Chinese ecosystem from 20 April to 1 May 2026.

Karla Crespo, CEDIA

Over two weeks, 29 academic leaders from 22 universities and one higher education institute took part in an academic immersion programme in China, held in the cities of Beijing, Shanghai, Hangzhou and Shenzhen. This tour helped to establish a platform for strategic exchange aimed at strengthening the international profile of Ecuadorian institutions and opening up new opportunities for academic, scientific and technological cooperation.

The itinerary included visits to universities, technology companies and hubs of innovation that are currently leading the way in digital transformation, scientific research and engagement with the productive sector. In total, the

delegation visited 16 strategic locations, including academic institutions, technology centres and innovation ecosystems.

Among the universities visited were Beijing Language and Culture University, China University of Petroleum, Renmin University of China, Shanghai International Studies University, Tongji University, Shanghai Jiao Tong University, New York University Shanghai, East China University of Science and Technology and Shenzhen Polytechnic University.

The Ecuadorian officials also gained first-hand insight into the work carried out by companies and technology centres such as iFLYTEK, Alibaba Group, Huawei and Unitree Robotics, where topics related to artificial intelligence, automation, cloud computing, supercomputing and digital services applied to education, industry and public administration were discussed.

One of the most significant aspects of the tour was the opportunity to analyse training models closely linked to industry and technological development. The visit to Shenzhen Polytechnic University provided a first-hand insight into how technical and technological education is integrated with processes of innovation, automation and dual training, incorporating practical work experience in companies into academic training.

Throughout the experience, five strategic pillars emerged that shaped the delegation's itinerary: structural internationalisation, applied research, digital infrastructure, artificial intelligence and university-industry links. These elements provided a basis for reflection on the current challenges facing higher education and on opportunities for adapting and implementing new practices within the Ecuadorian context.

The programme also helped to strengthen the international relationships of the participating institutions, creating opportunities for dialogue with rectors, vice-rectors, internationalisation managers and innovation leaders from the universities and companies visited.

For CEDIA, this experience reaffirms its commitment to fostering an academic network connected to the world, capable of forging strategic alliances, strengthening institutional capacities and promoting higher education aligned with the technological and scientific challenges of the future.

eduLACSeg: The defense force of Latin America's largest academic cybersecurity ecosystem

Now approaching its fifth anniversary and built on the foundations of a collaboration that has lasted more than 20 years – which, amongst other things, led to the creation of RedCLARA – the Regional Cybersecurity Group of the National Research and Education Networks (NREN) of Latin America and the Caribbean, eduLACSeg, is already proving its immense value. Find out more and discover how your institution can benefit from it.

Carlos González y María José López Pourailly

At some point in 2025, CERN's systems detected a threat. What followed was not the execution of a predefined process: via ELLALink — the submarine cable connecting Europe with Latin America, deployed as part of the BELLA programme — that information travelled from Switzerland to one of RedCLARA's servers in Latin America. From there, it was distributed to RNP, REUNA, RENATA, RedCONARE, RAU, CUDI and CEDIA – the NRENs of Brazil, Chile, Colombia, Costa Rica, Uruguay, Mexico and Ecuador (respectively) – which either used it or redistributed it to their institutions. Thus, a threat detected in Europe became, in real time, a warning to universities and research centres across Latin America.

This was made possible by the Regional Cybersecurity Group of the Research and Education Networks of Latin America and the Caribbean, eduLACSeg, which is a robust inter-NREN coordination mechanism for cybersecurity, coordinated by RedCLARA. This group is committed not only to the security of its networks and the academic and research organisations that form part of them, but also to its peer networks, to RedCLARA itself and, above all, to the region; this commitment is evident on a daily basis through the permanent working structure from which the main regional cybersecurity initiatives for the academic sector have emerged and are coordinated.

Its origins date back to 2019, when CUDI (Mexico) and CEDIA (Ecuador) began working together on security issues. In the following years, RNP (Brazil) and REUNA (Chile) joined the effort. On 2 September 2021, at the close of the TICAL Conference — the region's main annual gathering for academic networks — the executive directors of the four networks, together with RedCLARA, signed the Memorandum of Understanding that formalised the group and established its Co-ordination Committee. "RedCLARA and TICAL represent this space for collaboration, where we can learn and grow alongside other networks. The agreement to create the regional telemedicine network at TICAL2020 was a prime example, and now we have the agreement for the Cybersecurity group. We are delighted to be part of this initiative," said Juan Pablo Carvallo, Executive Director of CEDIA, on 2 September 2021.

Today, in 2026, as we prepare to celebrate the fifth anniversary of eduLACSeg's creation, the NIRs from Brazil, Chile, Ecuador, Mexico, Uruguay and RedCLARA are actively participating in the group's regional coordination and organisation. Furthermore, the academic networks of Colombia and Costa Rica take part in specific initiatives or on a regular basis.

"In the nearly five years since eduLACSeg was established, the progress has been remarkable. Collaboration is no longer limited to the region's NREN networks; with RedCLARA's support, agreements have been reached with organisations such as LAC4, Red Ciberlac, GÉANT, CERN and AMREN, amongst others, to develop projects, participate in initiatives and exchange cybersecurity threat intelligence. Progress is also evident amongst the region's NRENs; collaboration flows naturally, with the sharing of knowledge, tools, best practices, training and support for any cybersecurity incident," says Fernando Aranda, who, from CUDI, has been one of the group's key driving forces.

It is worth noting that the group has also benefited from the participation of ARIU (Association of University Interconnection Networks) from Argentina, as a guest in initiatives where its expertise has been particularly relevant.

"As is well known, the golden rule in cybersecurity is collaboration, and eduLACSec has undoubtedly enabled us to do just that. Within this framework, we have been able to address issues such as the exchange of technical and regulatory knowledge and experiences, as well as the formation of networks of trust between individuals—which is of the utmost importance in the field of cybersecurity, given the nature of the information handled and exchanged— it is essential to know the counterparts with whom you collaborate, so that, should an incident occur, we can provide rapid mutual support across academic networks", says Alejandro Lara of REUNA, highlighting the value of collaboration within this group.

At eduLACSeg, leadership is shared and rotates according to the nature of each initiative. RedCLARA and CUDI coordinate the group as a whole, RNP co-leads the maturity assessment process, and CEDIA guides the asset exposure assessments. This distribution is more than just a governance model; it is what makes it possible to move forward collaboratively, which is the group's defining value.

Sharing knowledge

Since 2020, the group has led the Strategic Cybersecurity Meetings at the TICAL Conference. Panels, technical sessions, workshops, CSIRT meetings: year after year, this forum has been the place where networks compare what they are observing, what they are doing and what they need.

Outside of TICAL, in October 2022 the group organised a series of four webinars featuring speakers from REUNA, CEDIA and CUDI, which reached the academic community across the region.

"The knowledge-generation efforts within eduLACSeg are fundamental

because they help to build a regional vision of the challenges facing cybersecurity. Beyond sharing technical information, these forums promote the exchange of experiences, collaboration between professionals and the development of new capabilities that benefit the academic and research community," emphasises Javier Valena from RAU.

This collaboration on raising awareness also extends to Europe. Since 2022, RedCLARA has been participating in

GÉANT's Cybersecurity Month, the European academic network's annual cybersecurity awareness campaign. In 2022, eduLACSeg contributed the expert insight of Emilio Nakamura, CISO of RNP, who delivered the presentation "Strengthening security and privacy culture in Latin American NRENs" to the global community.

For Erika Viviana Casas, Director of Technology and Infrastructure at RENATA, "participating in eduLACSeg means being part of a trusted community where we share experiences, best practices, lessons learnt and technical capabilities that strengthen the security of our member institutions. Thanks to this cooperation, the region's academic networks have been able to access high-impact initiatives, establish strategic partnerships with international organisations and respond in a more coordinated manner to the growing challenges of cybersecurity. A tangible example of this value is the collaboration established with CERN for the exchange of threat intelligence. Thanks to the coordinated efforts of eduLACSeg and RedCLARA, RENATA is able to receive early warnings about threats and attacks identified at an international level and share this information promptly with its member institutions, enabling them to strengthen their prevention and response mechanisms. This demonstrates how regional and international cooperation translates into concrete benefits for our academic communities."

And, speaking of cooperation, in 2025, as part of the continental AMREN initiative—a working group of networks in the Americas: RedCLARA (Latin America and the Caribbean), Internet2 (United States) and CANARIE (Canada)—and as part of Cybersecurity Month, on 7 October eduLACSeg shared its expertise with the Americas through the expert contribution of Jorge Merchán, from CEDIA, at the opening of the Ciberbridges webinar series. The session, which focused on the impact of deepfakes, social engineering and CSIRT response strategies, attracted more than 180 participants. The Ciberbridges series comprised four cybersecurity webinars running through to December; the session led by the CEDIA expert proved to be the most successful in terms of audience numbers. Jorge Merchán himself views this experience very positively: "Threats do not require visas nor do they recognise borders; faced with this, the question is not whether we collaborate, but how quickly and with how much confidence we are able to do so. Therein, for me, lies the true significance of Ciberbridges. The name says it all: it was not just a series of talks; it was a bridge connecting the knowledge from the north of the continent—Internet2, CANARIE—with the experience and challenges of the south, and it did so in Spanish, Portuguese, English and French, respecting the diversity of our region rather than erasing it. That is no minor detail: it democratises access to cutting-edge knowledge for institutions which, on their own, could never sit down to discuss Zero Trust or identity management with a CISO from a US university. For a network like CEDIA, which provides VOC, SOC, CSIRT and GRC services to a broad ecosystem of higher education institutions, initiatives like this multiply our capacity."

Surveying, measuring and improving

In 2023, the group coordinated the first regional cybersecurity survey aimed at higher education institutions, with support from Ciberlac (an IDB initiative). A total of 189 institutions from Chile, Uruguay, Brazil, Ecuador, Colombia, Costa Rica, Mexico and Guatemala took part, representing an estimated student population of two million people.

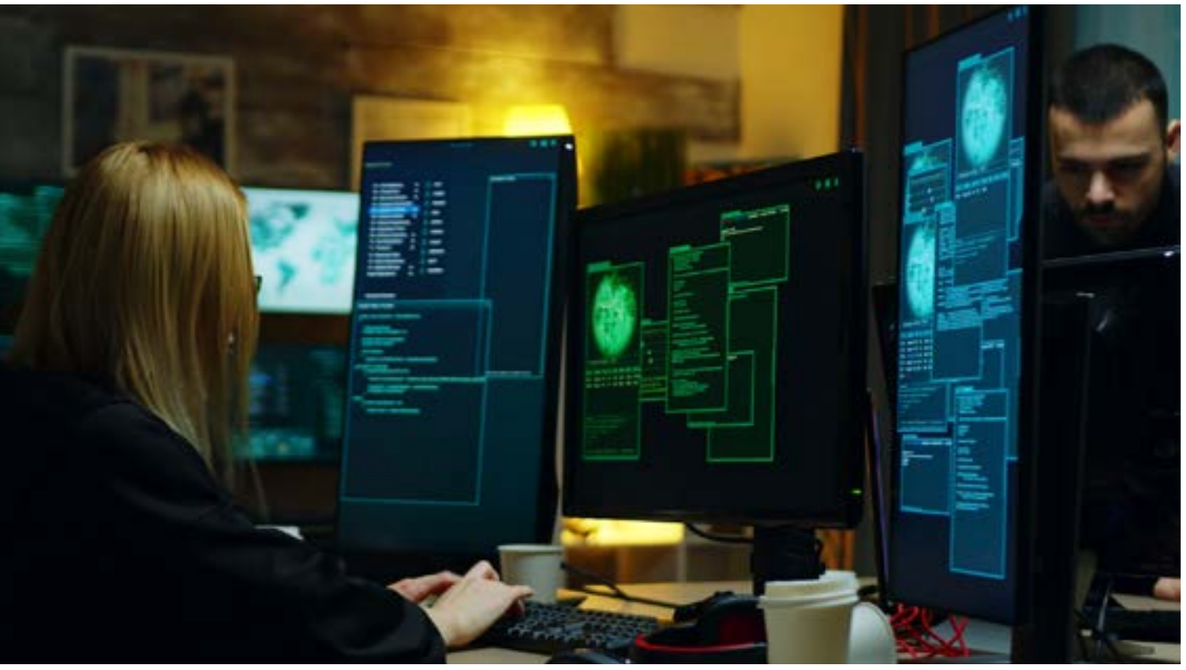
The results were revealing: 67 per cent of participating institutions did not have a security plan, and fewer than 20 per cent offered any academic programme in cybersecurity. The most critical skills gaps were concentrated in forensic analysis, secure development and vulnerability management, and 28 institutions that did not offer cybersecurity programmes expressed an interest in doing so — a clear sign of latent demand that the ecosystem could address.

Ivan Benevides, from RNP, explains the importance of carrying out these assessments through the survey: "Assessment is a crucial step that enables us to understand the current situation of each network and its scores, identifying the steps needed to achieve the desired strategic developments, transforming cybersecurity from a reactive cost centre into a proactive strategic pillar, and aligning technological protection with continuity objectives."

Using the survey's findings as a starting point, the group adopted GÉANT's Security Baseline framework to measure the cybersecurity maturity of national networks. The model assesses four organisational dimensions: policies, people, threats and operations, and enables results to be compared between networks in the region and with European networks that also implement it.

Ana Alves, an expert from the pan-European network, states that "for GÉANT, initiatives such as this are of fundamental strategic value. Collaboration with RedCLARA not only strengthens ties between regions but also significantly expands our ability to understand diverse cybersecurity challenges from multiple perspectives. This type of intercontinental cooperation enables the two-way sharing of knowledge, enriches approaches and accelerates the adoption of best practices that benefit all the communities involved".

The first phase, carried out in 2024 in collaboration with GÉANT's GN5-1 project (funded by the European Union), involved RNP, CEDIA and REUNA. In the second phase, currently underway in 2026, these three networks are supporting the others in their own assessment process.



The aim is for all networks to assess their maturity annually, compare themselves with one another and with Europe, and draw up joint improvement plans. The first consolidated results were presented at TICAL 2025, which showed a clear improvement in the maturity of the networks from the first phase and 100 per cent adoption of the framework by the region's networks.

A key conversation that spanned the Atlantic

Whilst the group was developing its first regional initiatives, a conversation at TICAL2021 opened up a new possibility. CERN was invited to take part in a conference session, where it presented its work on threat intelligence sharing. The meeting led to a regional collaboration agreement and the launch of an initiative that several networks began to implement in parallel. ARIU, the Argentine university network, made the fastest progress, and this practical leadership made it the benchmark that guided the other networks through the installation and roll-out process.

Today, the system operates as follows: CERN detects actual attacks or potential risks and sends this information, via ELLALink, to RedCLARA's central server. RedCLARA receives it and distributes it to the participating national networks, which in turn redistribute it to their institutions in accordance with their own policies. The protocol that makes all this possible is MISP — open-source threat intelligence sharing software — and the collaboration forms part of the CERN SAFER project.

In addition, the group has access to pDNSSOC, also developed by CERN, which enables threats to be blocked automatically via DNS. The system is available to networks wishing to implement it.

From sharing knowledge to building capacity, not just transferring it

A constant feature of the group's work is its commitment to building capacity within the networks and their institutions. This is clearly reflected in the collaboration with LAC4, the Cyber Competence Centre for Latin America and the Caribbean, funded by the European Union.

Through this partnership, the group has organised high-impact training programmes. In March 2024, RedCLARA and LAC4, with the support of eduLACseg, ran the course 'Training on the creation and operation of CSIRTs in the academic sector', which brought together 85 participants from nearly 60 organisations across 18 countries. The programme was led by an expert in Security Governance and included case studies presented by the NREN cybersecurity leads themselves, who are members of the Group: Jorge Merchán (CEDIA), Fernando Aranda (CUDI), and Ivan Tasso and André Landim (RNP). The aim was to empower the academic sector in both technical and legal and regulatory aspects related to the work of CSIRTs. The course had an immediate impact: the Universidad Autónoma del Carmen (UNACAR) in Mexico used what it had learnt to present a proposal to its senior management to set up its own CSIRT. The group has also organised a session for 56 participants on artificial intelligence and cybersecurity (2024) and a seminar on cybersecurity indices for NREN and institutions (January 2025).

At TICAL 2025, the group also ran a face-to-face and virtual workshop on how to plan and carry out cyber incident simulation exercises (tabletop exercises). The workshop was facilitated by a NATO specialist in collaboration with LAC4, and brought together 31 professionals from eight countries.

The approach was the same: rather than conducting a single exercise, the aim was to train the networks so that they could design and facilitate their own.

Danny Silva, an expert from RedCONARE, speaks very highly of the activity organised by eduLACSeg as part of TICAL in Costa Rica in 2025: "The workshop added immense value to the infrastructure of public universities, and the reception from RedCONARE was excellent, with a truly remarkable participation rate. What made the difference was the practical approach: the workshop didn't just stick to theory, but provided us with technical tools, methodologies and directly applicable material. The fact that we got to work on real-life scenarios (hands-on) was crucial for highlighting the current threat landscape. It made the urgency of standardising processes and the critical importance of operating within a joint framework to strengthen our security posture very clear to us."

What the system means

Let's go back to the beginning. When CERN detects a threat and that information reaches Latin American universities in real time, what is happening is not just a data transfer: it is the realisation of something that did not exist five years ago. What the group has built is a collective capability that amplifies what each network does on its own: threat intelligence arrives in real time via a trusted network that took years to build. This is possible because the networks decided to work together, and because there is a structure — eduLACseg — that turns those intentions into something concrete and sustainable.

That is what the group has built: not a centralised service, but a platform where the capacity of each network is multiplied by that of the others.

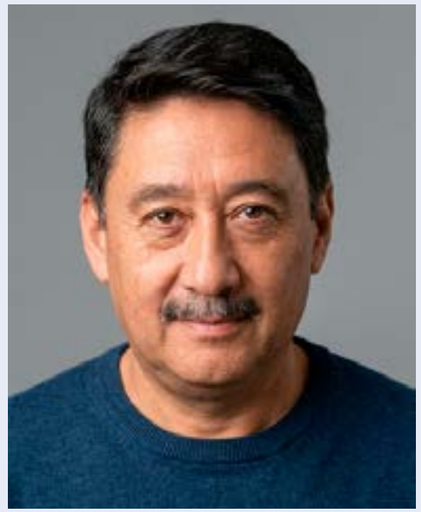
The group's cumulative work has generated concrete capabilities that are available to the networks and their institutions:

- Organisational maturity assessment using the GÉANT framework, with 100% of the networks using it to improve their cybersecurity posture.
- An operational threat intelligence-sharing system with Europe, backed by regional expertise in its implementation and use.
- The design and facilitation of cyber-incident simulation exercises, with several networks already trained to lead them.
- A network of partnerships with GÉANT, CERN and LAC4, with a track record of effective collaboration.

The Regional Cybersecurity Group is, above all, a collective endeavour of Latin America's academic networks. What exists today — the intelligence system connected to Europe, maturity assessments comparable with networks worldwide, incident response capabilities established across dozens of institutions, and spaces for dialogue and co-creation — was not designed by anyone from above: it arose from the decision by the NREN to work together and from the conviction that academic cybersecurity in the region is a shared responsibility.

For academic institutions in the region, belonging to an NREN that is a member of the group means access to this ecosystem: tools, training, threat intelligence and a community of practice that grows with every initiative. For external organisations and partners, RedCLARA and the group are the natural point of contact for any project seeking to engage with the Latin American academic sector on cybersecurity matters.

eduLACSeg, as explained by Fernando Aranda, CUDI, Mexico



Prior to 2018, the cybersecurity and incident response teams at the NRENs in Brazil, Ecuador, Chile and Mexico tackled the challenges involved in protecting the infrastructure of the NRENs themselves, as well as that of the institutions forming part of each one, in an isolated and ad hoc manner.

At that time, there was virtually no collaboration between the NRENs' cybersecurity teams; any that did exist was limited to very specific cases and took place on an informal basis.

Then, in 2019, we began holding meetings between the heads of the cybersecurity teams from some of the NRENs and realised that, together, we were much stronger in tackling cyber threats than we would be acting individually.

Following these meetings, we began to jointly develop and carry out several activities with our communities. These were primarily awareness-raising activities; however, although in some cases cybersecurity MOUs had been signed between NRENs, these initiatives still did not provide for implementation at a regional level, and this continued to hinder collaboration. This was because, if there was no signed MOU with the NREN you wanted to collaborate with, it was not possible to carry out the collaboration, or it continued to be conducted on an informal basis.

From 2021 onwards, and with the support of Red CLARA and its board of directors, a Memorandum of Understanding (MOU) on cybersecurity was signed between RNP, CEDIA, REUNA and CUDI. This MOU enables the cybersecurity teams of the NRENs to formally collaborate, leading to the creation of the eduLACSeg group.

In the past five years, since eduLACSeg was established, the progress has been remarkable. Collaboration now extends beyond the region's NRENs; with the support of RedCLARA, agreements have been reached with organisations such as LAC4, Red Ciberlac, GÉANT, CERN and AMREN, amongst others, to develop projects, participate in initiatives and exchange cybersecurity threat intelligence. Progress is also evident amongst the region's NRENs; collaboration flows naturally, with the sharing of knowledge, tools, best practices, training and support for any cybersecurity incident.

eduLacSeg is a group that prioritises collaborative work and supports the integration and growth of more cybersecurity teams within the NRENs in Latin America and among their members.

Through all its activities, eduLACSeg drives the development of the cybersecurity ecosystem in the region's education and research sectors.

This is undoubtedly one of the most valuable achievements of this group.

eduLACSeg, as described by Alejandro Lara, REUNA, Chile

As it is well known, collaboration is one of the fundamental principles of cybersecurity, and eduLACSec is undoubtedly a forum that has enabled us to put that objective into practice. Through this initiative, we have been able to exchange technical knowledge, experiences and best practices, which benefit all the communities involved, as well as explore regulatory aspects of common interest in greater depth. Above all, I would emphasise that this group has fostered the building of networks of trust between people, an essential element in cybersecurity. Given the nature of the information shared and the need to act swiftly in the event of an incident, getting to know and forging links with our peers from other academic networks is key to providing timely support and coordinating an effective response.

One of eduLACSec's greatest successes has been establishing and consolidating a regional cybersecurity community, through which we have carried out various initiatives to strengthen not only the security of each of the participating networks, but also that of our member institutions and the entire R&I ecosystem. At a technical level, I would highlight the adoption of GÉANT's Security Baseline to measure the cybersecurity maturity of national networks. This assessment has enabled us to understand our level of maturity, benchmark ourselves against others and design joint improvement plans tailored to the specific needs of academic networks.

eduLACSeg, as described by Javier Valena, RAU, Uruguay

I believe that the knowledge-generation efforts within eduLACSeg are fundamental because they help to build a regional vision of the challenges facing cybersecurity. Beyond sharing technical information, these forums promote the exchange of experiences, collaboration amongst professionals and the development of new capabilities that benefit the academic and research community.

I also value the fact that the knowledge generated stems primarily from the specific realities and needs of Latin America and the Caribbean. This enables us to tackle common problems from a perspective closely aligned with our context, fostering more practical and sustainable solutions.

In an environment where threats are constantly evolving, the collective generation of knowledge not only strengthens individual skills but also helps to foster a culture of cooperation and continuous learning, having a very positive impact on the growth of the regional cybersecurity community.

In my view, the group's greatest achievement has been to build a regional community based on trust and collaboration in cybersecurity.

Cybersecurity has one distinguishing feature: when a serious incident occurs, technological tools help, but what really makes the difference is knowing who to call, with whom to share sensitive information, and whom to trust. Building that human network between

universities, academic networks and specialists from different countries is difficult to quantify, but it is of enormous value.

I also believe it is important that eduLACSeg helps to establish the idea that cybersecurity in Latin American academia is a regional challenge rather than merely an institutional one. Most institutions in the region have limited financial resources, so collaboration is a strategic necessity. In this regard, the eduLACSeg group helps knowledge and capabilities to circulate between countries rather than remaining concentrated amongst a few key players.

eduLACSeg in the words of Erika Casas, RENATA, Colombia

Cooperation is eduLACSeg's core value and the reason why the group has established itself as a regional leader in cybersecurity for the academic sector. No single network, on its own, could develop the capabilities, tools and knowledge that we have collectively built today with the same speed and scope.

For RENATA, participating in eduLACSeg means being part of a trusted community where we share experiences, best practices, lessons learnt and technical capabilities that strengthen the security of our member institutions. Thanks to this cooperation, the region's academic networks have been able to access high-impact initiatives, establish strategic partnerships with international organisations and respond in a more coordinated manner to the growing challenges of cybersecurity.

A tangible example of this value is the collaboration established with CERN for the exchange of threat intelligence. Thanks to the coordinated efforts of eduLACSeg and RedCLARA, RENATA can receive early warnings about threats and attacks identified at an international level and share this information promptly with its member institutions, enabling them to strengthen their prevention and response mechanisms. This demonstrates how regional and international cooperation translates into concrete benefits for our academic communities.

Most importantly, this cooperation goes beyond the exchange of information: it becomes a shared regional capability that directly benefits universities, research centres and academic communities throughout Latin America.

I believe that eduLACSeg's greatest achievement has been to build a trusted regional community capable of transforming collective knowledge into concrete capabilities for academic networks and their institutions.

Thanks to the group's collaborative work, the region now has mechanisms for exchanging threat intelligence, processes for measuring and strengthening cybersecurity maturity, permanent training opportunities and a network of experts who openly share knowledge and experiences. All of this has enabled academic networks to be better prepared to prevent, detect and respond to security incidents.

One of the most significant achievements has been the launch of the regional threat intelligence-sharing ecosystem, developed in partnership with CERN and coordinated through RedCLARA. This initiative has enabled critical information on risks and attacks detected in other parts of the world to reach Latin American academic networks at an early stage, strengthening the ability of institutions such as those within the RENATA community to anticipate and respond to threats.

However, beyond specific tools and projects, the greatest achievement has been to demonstrate that regional cooperation generates tangible and sustainable results. eduLACSeg has created an ecosystem where the capabilities of each network are multiplied through joint efforts, strengthening the digital resilience of the academic sector in Latin America.

eduLACSeg, as explained by Jorge Merchán, CEDIA, Ecuador

Threats do not require visas nor do they recognise borders; an actor who strikes a university in Mexico today may be knocking on the door of an institution in Ecuador, Chile or Brazil tomorrow using the same technique. Faced with this, the question is not whether we collaborate, but how quickly and with how much confidence we are able to do so.

Therein, for me, lies the true significance of Ciberbridges, the initiative organised by RedCLARA in partnership with CANARIE and Internet2, to which I was invited to participate last year. The name says it all: it wasn't just a series of talks; it was a bridge, connecting the knowledge of the northern part of the continent—Internet2 and CANARIE—with the experience and challenges of the south, and it did so in Spanish, Portuguese, English and French, respecting the diversity of our region rather than erasing it. This is no minor detail: it democratises access to cutting-edge knowledge for institutions which, on their own, would never be able to sit down and discuss Zero Trust or identity management with a CISO from a US university.

26

For a network like CEDIA, which provides VOC, SOC, CSIRT and GRC services to a broad ecosystem of higher education institutions, initiatives such as this multiply our capacity. Each session represented talent that was developed, a best practice that was replicated, and a trusted connection that was forged. And in cybersecurity, that network of trust is, ultimately, our best line of defence. No country, no network, no institution can defend itself alone. Ciberbridges reminded us of that and provided us with the concrete platform to make it a reality.

If I had to choose just one thing as the most valuable of all the group's achievements, it would not be a course, a webinar or a document; it would be something less visible but far more profound: the group transformed security teams that were working in isolation – each tackling the same problems on their own – into a genuine regional community that knows one another, communicates and looks out for one another.

Before eduLACSeg, cybersecurity cooperation amongst the region's academic networks consisted of goodwill and loose contacts. Today, we have a structured framework to help our CSIRTs mature, to drive the creation of SOCs, to train our people through programmes such as the Security Baseline Bootcamp, and to bring the voice of the regional academic community to high-level forums, such as the EU-LAC Digital Alliance dialogues. We have moved from reacting individually to building resilience collectively.

The most valuable aspect of all this is trust. In our world, sharing a threat indicator or picking up the phone to ask for help during a crisis requires trusting the person on the other end of the line. That trust, built meeting by meeting, exercise by exercise, over almost five years, cannot be bought or improvised. For me, it is the most important asset the group has created, and the one that makes everything else work.

The group transformed security teams that used to work in isolation – each solving the same problems on their own – into a genuine regional community that knows, communicates with and looks out for one another. Before eduLACSeg, cybersecurity cooperation between the region's academic networks consisted of goodwill and loose contacts. Today it is a structured framework: we have a framework to help our CSIRTs mature, to drive the creation of SOCs, to train our people through programmes such as the Security Baseline Bootcamp, and to bring the voice of the regional academic community to high-level forums, such as the EU-LAC Digital Alliance dialogues. We have moved from reacting individually to building resilience collectively.

And the most valuable aspect of all this is trust. That capital of trust, built up meeting by meeting, exercise by exercise, over almost five years, cannot be bought or improvised. It is, for me, the most important asset the group has created, and the one that makes everything else work.

eduLACSeg, as represented by Iván Benevides, RNP, Brazil

Conducting the assessment carried out via the cybersecurity survey is essential for a number of strategic reasons:

Validation of each network's actual security posture: It enables a shift from assumptions to empirical data. In cybersecurity, what is not measured cannot be managed; this survey translates risk perception into tangible metrics, identifying critical gaps between theoretical policies and actual operations.

Optimisation and justification of resources: The results provide a clear roadmap for prioritising investments in infrastructure and training. By aligning the identified requirements with actual vulnerabilities, it ensures that financial and human resources are allocated where they will have the greatest mitigating impact.

Baseline for continuous improvement: It establishes an essential starting point (baseline). This not only allows the network's current maturity to be assessed against international standards but also serves to accurately measure the success and return on investment (ROI) of future security strategies that are implemented.

In summary: measurement is a crucial element that enables us to understand the current status of each network and its scores, identifying the steps required to achieve the desired strategic developments, transforming cybersecurity from a reactive cost centre into a proactive strategic pillar, and aligning technological protection with business continuity objectives.

From my perspective, the most valuable achievement of the group through this work has been to transform a discipline that is often abstract and reactive (cybersecurity) into a tangible, measurable and proactive strategy through the requirements gathering process.

Often, IT security is only addressed when something goes wrong. What the group has done in designing and implementing this measurement goes far beyond simply 'gathering data'; they have achieved some highly valuable milestones:

Building a bridge between the technical and the strategic: We have succeeded in translating vulnerabilities or technical requirements into the language of management and risk that any board of directors or committee can understand and assess.

Underpinning decision-making with evidence: Rather than designing strategies based on 'intuition' or the dictates of technological trends, the

group established a genuine, scientific baseline regarding the specific needs of the networks.

Establishing a replicable model: The rigour applied in the requirements gathering and survey not only solves a current problem but also leaves behind a structured methodology that can serve as a reference for future research or audits in the sector.

In the context of a publication, the value lies not solely in the numerical result we obtain, but in the rigour of the process we designed to arrive at it. This demonstrates that the group not only understands technology, but also how we are aligned – and committed – to the desire to improve together, supporting each country in its challenges to align with the continuity and maturity of the networks.

eduLACSeg, as represented by Ana Alves, GÉANT, Europe

Working with RedCLARA has been an extraordinarily enriching experience, a genuine opportunity for collaboration and mutual learning. The Security Bootcamp project came to life thanks to very close cooperation right from the start, particularly with Carlos, with whom it was a real pleasure to work due to his professionalism, dedication and constant commitment. This made the whole process not only productive but also very rewarding.

For GÉANT, initiatives such as this are of fundamental strategic value. Collaboration with RedCLARA not only strengthens ties between regions, but also significantly broadens our ability to understand diverse cybersecurity challenges from multiple perspectives. This kind of intercontinental cooperation enables the two-way sharing of knowledge, enriches approaches and accelerates the adoption of best practices that benefit all the communities involved.

At the same time, this collaboration also generates significant value for RedCLARA by facilitating access to international experiences, methodologies and reference frameworks that can be adapted to its regional context. Interaction with GÉANT and other networks helps to strengthen local capabilities, drive cybersecurity maturity and foster a culture of cooperation that multiplies the impact of initiatives across Latin America.

The assessments carried out through the survey and cybersecurity training activities are particularly valuable, as they provide a clearer, evidence-based insight into the maturity of the networks, enabling the identification of priorities, gaps and opportunities for improvement. For GÉANT, this is key to better targeting its initiatives, adapting its programmes and generating real and sustainable impact.

Furthermore, this type of collaboration reinforces one of GÉANT's essential pillars: building a global community that is more resilient and better prepared to face cyber threats. Working closely with partners such as RedCLARA not only multiplies the reach of our actions, but also fosters a sense of trust, alignment and shared purpose that is difficult to achieve in isolation.

It is undoubtedly a privilege for GÉANT to be able to contribute to the development of cybersecurity capabilities alongside RedCLARA and its member networks, and to continue strengthening a collaboration that delivers tangible, sustainable and long-term value to both regions.

eduLACSeg, as represented by Danny Silva, RedCONARE, Costa Rica

I believe that the cybersecurity workshop organised by eduLACSeg in San José as part of TICAL2025 added immense value to the infrastructure of public universities, and the reception from RedCONARE was excellent, with a very impressive participation rate. What made the difference was the practical approach: the workshop did not remain purely theoretical, but provided us with technical tools, methodologies and directly applicable material. The fact that we were able to work on real-life scenarios (hands-on) was crucial in highlighting the current threat landscape. It made it very clear to us how urgent it is to standardise processes and how critically important it is to operate within a joint framework to strengthen our security posture.

In my view, eduLACSeg's greatest contribution has been to consolidate communication channels and achieve genuine joint operational capability amongst the universities. At a technical and managerial level, it is all too easy for each institution to operate in isolation, but the group has enabled us to break down those silos. We have managed to exchange intelligence, harmonise strategies and recognise that tackling infrastructure challenges and vulnerabilities in a coordinated manner is far more effective than attempting to resolve them independently.

Carlos González: “eduLACSeg has the capacity to accommodate its diversity without losing cohesion”

As we have discovered through the voices of its members, eduLACSeg has evolved organically and is strongly based on collaboration. At RedCLARA, the person who has acted as the group’s coordinator is Carlos González, who is in charge of Innovation and the Service Portfolio; let’s hear his perspective.

From your experience, what has been the most difficult and the best aspect of establishing and maintaining the eduLACSeg group?

The most challenging aspect has been coordinating a regional agenda amongst organisations that operate with different mandates, timetables and capacities, without any one having formal authority over the others. Each National Network has its own institutional priorities, its own technical teams and its own decision-making processes. Building joint initiatives in this context, moving towards shared standards and maintaining the group’s coherence when teams change or when schedules become tight requires constant coordination – work that is not always visible but which makes everything else possible.

The best part has been seeing how the group developed its own dynamic. When one network helps another to set up a system without being asked, when they share information about an incident before it becomes a regional problem, when they jointly design a training programme that is more valuable than any one of them could offer on its own – that is what makes the whole effort

worthwhile. The group has developed something that is greater than the sum of its parts, and this has come about thanks to the trust built up over years of working together.

How do you assess the networks’ participation and involvement?

It has evolved in a way that strikes me as very genuine and organic. At the start, the group operated on the basis of goodwill and personal contacts. Today there is a self-organised structure; roles are defined by ability and initiative rather than by hierarchy; and there are measurable results that turn regional collaboration into concrete evidence of the value the group generates for each network and for their institutions. That is a significant change.

What I value most is that participation is not uniform, and that’s fine. Some networks lead specific initiatives because they have an advantage or needs in that area; others participate on a more regular basis; and some are in the process of consolidating their involvement. Rather than seeing this heterogeneity as a weakness, I view it as the natural way in which voluntary collaboration between autonomous organisations functions. What matters is that the group has the capacity to accommodate this diversity without losing cohesion, and that is something that was deliberately built in.

What are the next steps?

The group is marking the fifth anniversary of its formal establishment with a solid foundation and a work programme that no longer relies on external initiatives to move forward. What lies ahead is, on several fronts simultaneously, to build on what already exists and broaden our scope.

In terms of threat intelligence sharing, the aim is for all networks in the region to have the service up and running and to be able to systematically redistribute that intelligence to their institutions. We are working on this and wish to draw on the support of European partners who view the service very favourably and wish to join it.

Regarding maturity assessment, the process of closing the gaps identified in the second year is already underway across the seven networks. The next step is to launch the third assessment cycle, institutionalise the process to underpin concrete and fundable improvement plans, where appropriate, and assess the possibility of carrying out the assessment at the level of the member institutions of the National Networks.

In terms of training and capabilities, we are continuing to develop joint programmes to strengthen the Networks’ capabilities. The approach is always the same: rather than doing it ourselves, we teach others how to do it.

Finally, the group will have the opportunity to use the Cybersecurity Testbed, which is being developed through a co-investment model within the framework of the BELLA II project. It will enable its members to receive training and strengthen their institutions’ capabilities through controlled scenarios (CTF, incident response, forensic analysis) and to generate shared knowledge via the regional exercise library and the network’s own threat analysis.

What do you think is the group’s greatest contribution?

The greatest contribution is having transformed academic cybersecurity from an institutional problem into a regional challenge. Before the networks met to discuss CSIRTs – which led to their decision to create eduLACseg – each one was facing the same threats, developing the same capabilities and going through the same learning process. Today, that has changed: there is a shared intelligence system operating in real time; there is a common measurement framework that allows for peer-to-peer comparison and learning; and there is a community where members know one another, communicate and support each other when something goes wrong.

And, once again, what makes all of the above possible has a name that does not always appear in management reports: trust. Everything else – the systems, the protocols, the training – depends on the people on the other end of the phone or email being people you trust. That capital isn’t built in a workshop or through a signed agreement. It is built over five years of working together, and it is what makes the group difficult to replicate and almost impossible to replace.

CUDI signs an agreement with ENRICH LAC to strengthen cooperation in science, technology and innovation between Mexico and Europe

The University Corporation for Internet Development (CUDI) and the European Network of Research and Innovation Centres and Hubs in Latin America and the Caribbean (ENRICH LAC) have formalised an agreement aimed at strengthening multilateral cooperation in the fields of research, science, technology, innovation and entrepreneurship between Europe, Latin America and the Caribbean.

Based in São Paulo, Brazil, ENRICH LAC is a private, non-profit organisation that acts as a strategic bridge between the two regions, facilitating access to new international markets for researchers, academic institutions and innovative entrepreneurs. CUDI manages Mexico's National Research and Education Network (NREN), which connects the country's universities, institutes and research centres with similar networks in Europe, Asia, Oceania, North America and Latin America.

The agreement recognises the strategic role of the Support Centres for the Adoption of New Markets, organisations that assist researchers and entrepreneurs in their international expansion through specialised services such as advice on local business culture and practices, co-working spaces, administrative support for visas and registrations, regulatory guidance, and facilitating contacts with the scientific and business communities in each country.

Beyond these specific services, the partnership's underlying aim is to foster strong alliances between Europe and Latin America in the fields of science, technology and innovation, contributing to the development of sustainable and competitive businesses, and promoting both applied research and high-impact entrepreneurship.

Strategic collaboration with a global reach

For CUDI, this agreement represents an opportunity to expand the capabilities of its network and offer its member institutions new avenues for international engagement. Through its exclusive links with regional networks worldwide, the Mexican NREN becomes a key hub for connecting Mexico's scientific and technological talent with the European innovation ecosystem that ENRICH LAC facilitates.

The partnership, which is non-exclusive and involves no financial obligations, will initially run for 12 months, with the possibility of extension as the relationship between the two organisations develops.

This agreement reaffirms CUDI's commitment to the internationalisation of Mexican science and to building collaborative networks that foster the country's development within the global knowledge economy.

REUNA becomes the first academic network to join the IOWN Global Forum

The Chilean network joins a global community of more than 170 organisations working to drive the networks of the future through innovation in optical, wireless and distributed processing technologies.

Carolina Muñoz, REUNA

IOWN (Innovative Optical and Wireless Network) is a technological initiative led by NTT (Nippon Telegraph and Telephone Corporation), in collaboration with companies and research centres around the world. Its aim is to redefine the communications infrastructure of the future by integrating advanced optical networks, next-generation wireless technologies and intelligent distributed processing systems, with a view to moving towards a more sustainable and environmentally friendly society.

To drive this vision forward, the IOWN Global Forum was established – a community bringing together more than 170 leading organisations from the global technology ecosystem, working to accelerate innovation and the adoption of photonics-based technologies. REUNA has just joined this international collaborative space, becoming the first research and education network to form part of this initiative.

As Paola Arellano, REUNA's executive director, explained: "Chile's inclusion in this initiative, through REUNA, will enable us to be part of the global discussion on the challenges ahead in the field of digital infrastructure, such as the adoption of technologies that improve energy efficiency and network performance. Furthermore, it will allow us to participate in continent-wide experiments to test these technologies and promote their implementation."

Arellano added that moving towards more sustainable, high-performance digital infrastructure will require a joint effort from the entire technology ecosystem. "We hope that, following this inclusion, we can bring together the national research community to join us and work collaboratively on developing new solutions."

For his part, Katsuhiko Kawazoe, Chair of the IOWN Global Forum and Executive Vice-President of NTT, stated that this partnership strengthens the international cooperation that has historically existed between scientific and academic institutions on both sides of the Pacific. "There is a long history of research and development between Chile and Japan. With REUNA's participation in the IOWN Global Forum, we can take that collaboration to a new level," he noted.

Background to a pioneering collaboration

The relationship between REUNA and NTT dates back to the early 2000s, when both organisations took part in a pioneering experiment that enabled

a Codelco robotic arm, located in Chile, to be operated remotely from Japan. This milestone represented an unprecedented global collaboration for the country, bringing together the research and education networks of Chile, Latin America, the United States and Japan.

Years later, in collaboration with the National Laboratory for High-Performance Computing (NLHPC) and using NTT's optical technology, the metropolitan photonic ring was deployed. This advanced digital infrastructure enabled the interconnection of computing centres at various universities in Santiago, creating a significant space for technological experimentation and learning.

Opportunities to drive innovation and experimentation

The inclusion of REUNA in the IOWN Global Forum opens up new opportunities for collaboration, including the possibility of implementing technology pilot schemes alongside Chilean institutions.

According to Kawazoe, academic networks play a key role in bringing innovation closer to society, democratising access to state-of-the-art solutions. "Innovation does not reach society quickly. In this regard, networks such as REUNA are very important, because their participation in initiatives such as the IOWN Global Forum enables academic and research organisations to utilise these types of networks and technologies".

The forum's chair also highlighted REUNA's understanding of the scientific and academic community, which will facilitate the development of new technological solutions, in collaboration with NTT, that are tailored to the needs of these users.

In a context where large-scale scientific projects — such as astronomical observatories or computing centres for artificial intelligence — generate massive volumes of data, which must be transferred within seconds to processing centres distributed across different parts of the world, strengthening networking becomes essential. Having more robust, resilient and efficient digital infrastructures is therefore an essential challenge for the advancement of science and the generation of new knowledge.

For further information, visit:
https://www.rd.ntt/e/iown/
https://iowngf.org/

RNP strengthens international cooperation for the structuring and development of AngoREN

RNP participated in the AngoREN National Roadshow 2026, the National Education and Research Network of Angola, on May 11th in Luanda and May 13th in Benguela, at the invitation of the Angolan Ministry of Higher Education, Science, Technology and Innovation (MESCTI), within the scope of the Higher Education, Science and Technology Development Project (TEST). The event brought together representatives from the government, higher education institutions, research centres and strategic partners, including telecommunications companies, to present AngoREN and the Executive Roadmap for the Digital Transformation of Higher Education.

RNP

The TEST Project The TEST Project is an initiative of the Angolan Government that aims to improve the quality of students entering higher education, update programs in strategic areas, and strengthen the management of the sector, including AngoREN

itself. With funding of $200 million from the World Bank and a direct impact on more than 185,000 beneficiaries by 2028, the project operates throughout the national territory, with initial interventions in the provinces of Bengo, Huambo, Huíla, and Uíge.

The meeting marked a decisive moment for the transformation of higher education in Angola, promoting strategic alignment, institutional mobilization, and concrete preparation of institutions for a new reality—more digital, more connected, and more integrated.

At the heart of this process is AngoREN, a national infrastructure for education and research that will enable:

- Connecting higher education institutions and research centres;
- strengthen academic connectivity and offer other related services;
- to broaden access to knowledge and innovation;
- to integrate Angola into international education and research networks.

In a complementary manner, the Digital Transformation Roadmap for Higher Education, within the context of the TEST Project, establishes guidelines for modernizing the sector, addressing technological challenges, and strengthening institutional capacities, creating conditions for higher education to act as an engine for the scientific, technological, and socioeconomic development of the country.

Representing RNP at the event were the Director of Services and Solutions, Antônio Carlos Fernandes Nunes, the Director of Engineering and Operations, Eduardo Grizendi, and the Governance and Management Manager, Pilar de Almeida. They shared the Brazilian experience in structuring and operating a national education and research network, addressing topics such as modelling, structuring and offering services, programs and projects with an impact on public policies,

training, governance, open innovation, infrastructure, and institutional relations.

RNP as a platform for the development of teaching and research

In his presentation, Antônio highlighted RNP as a strategic platform for the technological development of education and research in Brazil, emphasizing its role as a national, non-profit academic network focused on generating public value.

Data was presented on the organization's reach, connecting thousands of institutions, campuses, researchers, and students through a robust fibre optic infrastructure and advanced digital services. The presentation also addressed the historical evolution of the network, from the introduction of the internet in Brazil to its current role in digital transformation, collaborative innovation, and support for public policies in science, technology, and education.

The presentation highlighted RNP's experience in research, development and innovation (R&D&I) programs, in offering specialized digital services and in building collaborative ecosystems, elements considered relevant to inspire and support the consolidation of AngoREN.

"RNP's participation reinforces the strategic role of Brazil-Angola cooperation in strengthening the digital, scientific, and educational capabilities of both countries. By sharing its trajectory as a national academic network responsible for supporting the digital transformation of teaching and research in Brazil, RNP presents a consolidated model of action based on advanced infrastructure, digital services, innovation programs, and the articulation of collaborative ecosystems focused on generating public value and supporting public policies. Contributing to the consolidation of AngoREN means supporting the construction of an academic network capable of boosting teaching and research in Angola, based on the sharing of experiences in institutional modelling, structuring of services, development of impactful programs, and skills training. This rapprochement strengthens South-South cooperation and reaffirms RNP's commitment to international cooperation in the development of collaborative digital environments for education, science, and innovation," highlighted Antônio Carlos Fernandes Nunes.

The importance of partnerships in deploying robust optical infrastructures

Grizendi's presentation addressed RNP's strategy for deploying and sustaining its optical infrastructure – backbone and metropolitan networks – through partnerships with providers and operators, highlighting the construction of state and regional information highways in the country, always in partnership and sharing infrastructure with market operators and ISPs.

In the context of academic networks, the Director of Engineering and Operations presented RNP from the perspective of open innovation, capable of connecting universities, research centres, companies, startups, and government. He also highlighted how the organization's infrastructure—including fibre optics, data centres, and experimentation environments—can support applied research projects, technological development, and new business models, contributing to the strengthening of national innovation systems.

"A robust infrastructure for an academic network must be continuously pursued to ensure it is always available to researchers and educators, not only for their daily use, but also and especially to meet their ICT demands for scientific and technological research, and educational activities in higher education. And this needs to be done boldly, but always with concern for its sustainability," emphasized the Director of Engineering and Operations.

Governance, relationships, and institutional model of RNP

In the presentation led by Pilar de Almeida, the focus was on governance and the institutional relationship model of RNP. Pilar presented the RNP System as a collaborative community formed by educational, research, and innovation institutions, guided by principles such as neutrality, transparency, cost sharing, and technical excellence.

The organization's governance structure, its councils and committees, as well as the mechanisms for interaction with the academic community, government agencies, and strategic partners were detailed. She also emphasized the importance of networking, institutional cooperation, and strategic alignment to ensure sustainability, legitimacy, and long-term impact—aspects considered fundamental to the structuring of AngoREN.

"Sharing ideas about governance, opportunities, and challenges of sustainability for academic networks, in their different contexts and characteristics, is a very enriching experience! Furthermore, I noticed a strong alignment between the ministry team and the academic community with the AngoREN initiative. I have high expectations for the continuation of our cooperation," stated Pilar.

Participation in AngoREN's National Roadshow 2026 reinforces RNP's commitment to international cooperation, the exchange of experiences, and the strengthening of academic networks as strategic instruments for the digital transformation of education, science, and the promotion of innovation around the world.

SPIDER publishes a Position Paper outlining new strategic pathways to leverage bi-regional connectivity between the EU and Latin America and the Caribbean

In March 2026, the European SPIDER project released the document "Pathways for the Exploitation of the BELLA Infrastructure", a Position Paper presenting recommendations and priority areas to promote the strategic use of the digital connectivity linking Europe with Latin America and the Caribbean, now enhanced by the BELLAII project.

María José López Pourailly

The report is the result of two years of data collection, surveys, expert dialogues and collaborative work between stakeholders from both regions. SPIDER — an initiative funded by the European Union and involving the academic networks RNP in Brazil, REUNA in Chile, RedCONARE in Costa Rica, and CEDIA in Ecuador, alongside European organisations — seeks to strengthen bi-regional digital and scientific cooperation, particularly in contexts of growing demand for data exchange, shared infrastructure and advanced technological capabilities.

Beyond connectivity: a strategic asset for cooperation

One of the document's main conclusions is clear: connectivity, on its own, is not enough. Whilst the connectivity infrastructure enhanced by the BELLAII project provides a solid technical foundation, the report notes that it is often used merely as a service ( ), rather than being recognised as a key strategic asset for international cooperation.

The analysis also highlights that digital collaboration between the two regions remains fragmented and heavily reliant on one-off projects, which hinders the development of sustainable initiatives.

Furthermore, gaps persist in capabilities, funding and national infrastructure, limiting a more equitable adoption of services across Latin America and the Caribbean.

In this context, the Position Paper calls for the integration of this advanced connectivity into the political priorities and bi-regional digital dialogue, promoting an ongoing public commitment that guarantees its open, reliable and non-commercial nature.

Priority areas for strategic use

The document identifies six areas where the coordinated use of this infrastructure can generate the greatest impact, particularly in scenarios where cross-border cooperation is essential:

- Data-intensive research: facilitating secure and rapid access to large volumes of scientific information.
- Artificial intelligence and advanced computing: enabling joint experimentation and the development of innovative solutions.
- Cybersecurity: promoting shared capabilities in the face of growing threats.
- Satellite data and Earth observation: supporting environmental, climate and agricultural monitoring.
- Virtual research environments: enabling remote collaboration between laboratories and research centres.
- High-performance computing (HPC): expanding access to advanced processing resources that many institutions cannot sustain on their own.

These areas reflect key sectors for scientific development, technological innovation and knowledge generation in an increasingly interconnected global environment.

Recommendations for sustained cooperation

The document proposes five lines of action to maximise the impact of this bi-regional connectivity:

1. Recognising it as a shared asset within EU–LAC digital cooperation.
2. Link its use to specific policy priorities and the outcomes of the bi-regional dialogue.
3. Prioritise long-term initiatives over isolated projects.
4. Promote inclusion and balance in access and use in both regions.
5. Ensure a sustained public commitment that preserves its value as open and reliable infrastructure.

A key step towards deeper collaboration

With this document, SPIDER provides evidence and strategic guidance to move towards more structured and lasting cooperation between Europe and Latin America and the Caribbean.

The Position Paper not only reinforces the importance of connectivity enabled by the BELLAII project as a technological enabler, but also highlights its role as a catalyst for innovation, open science and international collaboration for the benefit of both regions.

The full report is available to the public and includes a detailed set of analyses and recommendations aimed at policymakers, academic institutions and stakeholders in the digital ecosystem.

Download it here

Smart Agro RAF LATAM: Blockchain for traceability in family farming in Latin America

Family farming forms the basis of food security in Latin America, but faces persistent challenges in terms of transparency, traceability and access to higher-value markets. Smart Agro RAF LATAM is a regional collaborative initiative which, supported by the BELLA II Early Adopters Blockchain programme – run between September and December 2025 – demonstrates how the advanced digital infrastructure of RedCLARA and the national research and education networks (NRENs) that comprise it enables innovative solutions with a direct impact on rural communities.

María José López Pourailly

More than 60 million people in Latin America and the Caribbean live on rural properties, which account for 80% of properties in the region. According to Smart Agro RAF LATAM studies, “in Colombia, 74% of agricultural units fall under the concept of Peasant, Family and Community Agriculture (ACFC). In Brazil, family farming accounts for 77% of rural holdings and forms the economic basis of 90% of municipalities with up to 20,000 inhabitants.” There is no need to delve deeper into these figures to understand that, from Mexico to Patagonia, family farming is crucial for societies and economies. This is why food security becomes so vital.

But what do we mean when we say “food security”? According to the World Bank: “Food security is achieved when all people have physical, social and economic access to sufficient, safe and nutritious food at all times to meet their nutritional needs and lead an active and healthy life.”

Raising the profile and value of family farming

It goes without saying: in Latin America, millions of small-scale producers account for a large part of food production. However, the lack of reliable traceability and certification systems limits their access to competitive markets and reduces the added value of their products. This gap affects producers, consumers and the institutions that require guarantees of origin, quality and, of course, sustainability within agri-food chains.

To overcome this challenge, Smart Agro RAF LATAM proposes a blockchain-based platform that enables the recording and verification of every stage of the production process, through the issuance of digital assets (tokens) representing agricultural products or certifications.

The solution is built on the following pillars:

- Smart contracts that automate traceability.
- Verifiable digital credentials for producers.
- Accessible interfaces that reduce technological complexity.
- Modular architecture that facilitates regional scalability.

The combination of these pillars results in greater transparency, improved market positioning and digital empowerment for producers.

Why did the members of Smart Agro RAF LATAM decide to apply for the blockchain testbed through BELLAII’s Early Adopters Programme? The answer is provided by the project leader, Rodrigo Mansilha, Prof. Dr. and Coordinator of Research, Development and Innovation in Information Technology and Artificial Intelligence at the Federal University of Pampa: “We developed a solution aimed at the Brazilian public. We saw the call for proposals as an opportunity to validate our idea (both in terms of users’ problems and our proposal to solve them) in Latin America. Without a doubt, it was the network of contacts that allowed us to take our project further and reach more people. The technical infrastructure enabled us to validate our technical decisions.”

Regional collaboration

One of the most distinctive features of Smart Agro RAF LATAM is its deeply collaborative nature, as it brings together researchers and specialists from:

- Brazil: Federal University of Pampa, Federal Institute of Rio Grande do Sul (linked to and supported by the initial project -ProRAF (https://proraf.com.br/)- which gave rise to Smart Agro RAF LATAM, via RNP through its IlÍADA initiative https://www.rnp.br/noticias/confira-os-4-grupos-de-trabalho-selecionados-na-segunda-chamada-publica-do-projeto-iliada/).
- Colombia: University of Antioquia.

The project is led, as explained above, by Rodrigo Mansilha (Brazil), with a multidisciplinary team specialising in computing, blockchain and information security, working in collaboration with academic and local stakeholders in Colombia.

Furthermore, the pilot directly involved nine farming families in Antioquia and Quindío, in Colombia, integrating local knowledge with technological development.

This collaboration between countries, institutions and communities reflects the potential of the Latin American digital ecosystem to co-create solutions with local relevance.

Progress via BELLA through the Early Adopters Blockchain programme

Smart Agro RAF LATAM made significant progress in its challenge thanks to the enabling environment provided by BELLAII and RedCLARA through the Early Adopters Blockchain programme. This allowed the team to access strategic mentoring, regional visibility and a structured framework for the development of the pilot.

"We already had experience with our Brazilian infrastructure maintained by RNP. We felt that the testbed documentation was very important, even for overcoming language barriers," says Rodrigo Mansilha. The specialist notes that participating in BELLAII's Early Adopters Blockchain Programme and using the testbed was a valuable contribution to Smart Agro RAF LATAM, as "access to another large-scale testing environment helps to reinforce scientific results, beyond the technical validation of the integration".

Using the blockchain testbed enabled the project's development team to:

- Test the solution in a distributed, high-performance environment.
- Validate security, scalability and performance.
- Simulate real operating conditions at a regional level.

In their own words, as recorded in the final report at the conclusion of the Early Adopters Blockchain experience developed within the BELLAII framework: "The programme and the testbed were fundamental in transforming a conceptual idea into a technically valid and strategically focused pilot, allowing us to test in a real-world environment and align with RedCLARA's vision."

As the team itself noted, beyond the technical aspects, the unique value lies in RedCLARA's advanced connectivity, which integrates capabilities, people and knowledge across Latin America. This environment facilitates joint experimentation and accelerates the maturation of solutions that transcend borders.

Real impacts for society

The impact of Smart Agro RAF LATAM is tangible and multifaceted. For producers (farming families), it offers greater autonomy over their data, improved regulatory compliance, and potential access to premium markets. For consumers, the benefits lie in transparency regarding the origin of food, and confidence in its quality and sustainability. For governments and institutions involved in agriculture and economic development, the added value lies in the development of more efficient auditing tools and better-designed public policies. Finally, for the region, the highly positive impact lies in driving the digital transformation of agriculture, reducing technological gaps, and fostering regional integration based on innovation; in the long term, this will also lead to cost reductions and improved food security.

Projection and scalability

Smart Agro RAF LATAM will move towards developing operational pilot schemes with agricultural cooperatives, integrating with commercial traceability systems, and expanding into new production chains and countries. The aim is to establish an ecosystem in which smallholder farmers can compete on a level playing field, supported by world-class technology and an unprecedented regional collaboration network.

More than technology: an ecosystem that enables solutions

The case of Smart Agro RAF LATAM demonstrates that the true value of BELLAII lies not solely in the technology, but in the ability to create conditions for effective collaboration.

The blockchain testbed, the RedCLARA infrastructure and the coordinated work of the RNIE form an environment where:

- Ideas can be tested under real-world conditions.
- Teams can collaborate without geographical barriers.
- Solutions can be scaled up regionally.

As a result, Smart Agro RAF LATAM validates a technology, but more than that, it paves the way for a replicable innovation model for Latin America and the Caribbean.

The blockchain testbed – a collaboration between RedCLARA and LNET – is the region's most robust public-permissioned infrastructure for the secure experimentation of Web 3.0 solutions. It is an advanced environment that drives the development, validation and scaling of decentralised solutions, designed for those seeking to carry out projects in a regulated, secure environment that complies with international standards. Through this testbed, universities, research centres, start-ups, governments and businesses can design, test and optimise blockchain applications such as digital credentials, supply chain traceability, digital identity and smart contracts, without incurring transaction costs and without the need for their own infrastructure. Further information at: https://www.bella-programme.eu/pt/results/testbeds/blockchain-testbed-ii.

SUBMERSE concludes its journey and looks ahead to the future of underwater sensing in Europe

From 15 to 17 April 2026, the SUBMERSE project held its final event at the University of Copenhagen, Denmark, bringing together consortium partners, scientific communities, infrastructure operators and industry representatives to share results and discuss the future of underwater fibre-optic sensing.

María José López Pourailly

Funded by Horizon Europe, SUBMERSE demonstrated the potential of repurposing submarine fibre-optic cables as scientific instruments capable of providing near-real-time data for seismology, oceanography, marine biology and tsunami monitoring. RedCLARA is one of the 24 members of the consortium driving this initiative, helping to strengthen international scientific cooperation and the strategic use of advanced research infrastructures.

During the meeting, participants reviewed progress made at various deployment sites across Europe and agreed on the need to continue building shared frameworks for collaboration and data governance to scale these capabilities at a pan-European level. The conclusion of the project leaves a solid foundation for new scientific applications and for greater integration of fibre-sensing into the research infrastructure ecosystem.

Alongside the final event, the project published the Policy Brief 'Opportunities and policy perspectives of subsea fibre-sensing technology', with recommendations for European Union policymakers on how to harness the potential of this technologymo aproveitar o potencial dessa tecnologia.

Read the full article and download the Policy Brief here.


RedCLARA
Cooperación Latino Americana
de Redes Avanzadas