CENTRO DE NOVAS TECNOLOXÍAS DE GALICIA

SANS

Case Study:

Galicia builds regional cyber resilience through public SANS training programme

Interview with **Carlos Vázquez Mariño**

Executive Summary

This case study describes how the regional government of Galicia, Spain, built cyber resilience through a strategic public cybersecurity training programme. In 2024, as Spain rose to fifth globally for ransomware attacks, the Centro de Novas Tecnoloxíasde Galicia (CNTG) launched an initiative offering SANS training to citizens across the region, including both employed and unemployed participants.

The programme began with a systematic needs assessment led by Amtega, Galicia's Agency for Technological Modernisation. Working closely with public- and private-sector stakeholders, Amtega identified the most critical cybersecurity skills gaps across the regional workforce. Through Spain's public procurement process, SANS Institute was selected as the training provider based on its global reputation and the value of its industry-recognised GIAC certifications.

In 2024, the first cohort saw 20 students complete SEC504 and FOR508, achieving satisfaction scores above 9/10 and reporting measurable career advancement, including salary increases. Local companies also benefited: newly certified employees enabled them to qualify for tenders requiring certified cybersecurity professionals.

The programme's early success has established a sustainable model in which public investment in cybersecurity education delivers measurable returns across the regional economy. Plans are already underway to expand the curriculum to include SEC556 and FOR572.

Galicia's collaborative approach demonstrates how regional governments can simultaneously address immediate cybersecurity skills shortages and build long-term cyber resilience. This initiative offers a replicable blueprint for other autonomous regions and governments worldwide seeking to strengthen their cybersecurity posture through accessible, high-quality training.

Carlos Vázquez Mariño

Director, Centro de Novas Tecnoloxías de Galicia (CNTG)

Regional Ministry of Employment, Trade and Emigration, Xunta de Galicia

Carlos Vázquez holds a degree in Computer Science from the University of Coruña and is a career civil servant in the Secondary Education Teachers' Corps (Computer Science). He served as Deputy Director General of Information Systems at the Department of Education (2009–2012); Director of the Sectoral Technological Solutions Area at the Galician Agency for Technological Modernization (AMTEGA) (2012–2020); Deputy Director General for Vocational Training at the Department of Education (2020–2022); and has been Director of the CNTG since 2023.

GALICIA BUILDS REGIONAL CYBER RESILIENCE
THROUGH PUBLIC SANS TRAINING PROGRAMME

"The professionals who complete the SANS training gain a ***competitive edge****, making the* ***investment worthwhile****."*

The digital transformation has swept across Spain's autonomous regions, but few have approached cybersecurity workforce development as strategically as Galicia. In 2024, Spain experienced a significant increase in cyber threats, ranking fifth place globally in ransomware attacks, with 58 incidents reported in the first half of the year, a 23 percent increase compared to 2023[1].

Against this backdrop, the regional government of Galicia launched an ambitious public cybersecurity training programme that offers professional development opportunities to citizens across the region. The programme sets a new standard for how governments can strengthen regional cyber resilience through strategic public investment in skills development.

The Centro de Novas Tecnoloxías de Galicia (CNTG) is one of the Galician government bodies leading this initiative. CNTG is a public vocational training centre under the Galician regional government's Department of Employment, serving both employed and unemployed citizens seeking opportunities in the technology sector. The centre's mission extends beyond traditional IT training. As its director, Carlos Vázquez, describes, the aim is to build a dynamic, technically prepared professional collective that can meet the cybersecurity challenges facing this autonomous community in northwestern Spain.

Identifying Regional Need

CNTG's evolution into cybersecurity training did not happen in isolation. The centre's broader mission to build technical expertise intersected with a growing regional need identified by government partners. This convergence would ultimately reshape how Galicia approaches cybersecurity workforce development.

The catalyst came through Amtega, "*a separate unit within the Galician regional government structure that manages the policies and actions of cybersecurity in Galicia, particularly in public administrations*," explains Vázquez. The Agency for Technological Modernisation of Galicia (Amtega) is attached to the Ministry of Finance and Public Administration of the Xunta de Galicia, with primary objectives including defining, developing, and implementing cybersecurity strategies, policies, and management for the regional public sector.

Amtega's approach to identifying cybersecurity training needs relies on direct engagement with the region's professional community. "*Through ongoing conversations with cybersecurity stakeholders across both public and private sectors, Amtega identified specific skill gaps affecting regional cyber resilience*", Vázquez notes. This systematic consultation revealed demand for specialised cybersecurity courses that would make a meaningful difference for regional professionals.

Making the Business Case

The decision to partner with SANS Institute to provide the cybersecurity training was driven by clear strategic reasoning. "*In determining the need for SANS training, it was taken into account that its training is prestigious and recognised by the entire market, both by cybersecurity professionals and by companies in the sector,*" Vázquez explains. A key factor in SANS's training is that courses come with opportunities to earn GIAC certifications. These industry-recognised credentials validate specific cybersecurity competencies. This certification component would prove crucial to the programme's success.

The business case for investing in premium cybersecurity training wasn't simple to make. "*It is quality training, but significantly more expensive than others*," Vázquez acknowledges. However, his argument to regional leadership focused on long-term competitive advantage: "*The professionals who complete this training gain a competitive edge making the investment worthwhile. While the courses may be more expensive than alternatives, they equip our professionals with specialised qualifications and certifications that open doors in the national and international job market.*"

[1] https://cds.thalesgroup.com/en/hot-topics/spain-fifth-country-most-ransomware-threats-2024

Measuring Programme Success

CNTG's cybersecurity programme is open to all citizens of Galicia, whether employed or unemployed. However, as Vázquez explains, participants are primarily "*professionals from the Galician IT sector who are dedicated to cybersecurity.*"

The response from participants has been overwhelmingly positive. "*At the end of each course, we do an evaluation. The students value the quality of that training, and this evaluation has been very positive, scoring higher than 9 out of 10,*" reports Vázquez. The qualitative feedback is equally telling: "*The feedback we recieve from participants is that having access to this training in Galicia is a privilege.*"

> *"Certification is significant to individuals, as companies recognize that those who earn it have advanced cybersecurity competencies."*

CNTG measures success through three key metrics: demand levels, immediate participant satisfaction, and six-month career impact assessments. The results validate the investment, with the GIAC certification component delivering particularly strong returns.

The market recognition of GIAC certifications has created a virtuous cycle. Both professionals and employers understand their value, driving ongoing demand.

"*Certification is significant to individuals, as companies recognize that those who earn it have advanced cybersecurity competencies. Some individuals have improved professionally within their company or have obtained job opportunities elsewhere and achieved an improvement in their professional career,*" Vázquez explains.

Beyond career advancement, individuals holding GIAC certifications have enabled their companies to qualify for tenders or projects that were previously inaccessible. The certifications serve as concrete proof of skills and have opened new business opportunities. As Vázquez notes, certifications have become essential in competitive bidding: "*In many tenders, they require specific certifications for the project. If you cannot prove that team members hold these certifications, you are automatically disqualified.*"

Broader Strategic Implications

The programme's success has led to significant expansion. Starting in 2024 with 20 students annually receiving training in **SEC504 (Hacker Tools, Techniques, and Incident Handling)** and **FOR508 (Advanced Incident Response, Threat Hunting, and Digital Forensics)** training, CNTG is evaluating adding **SEC556 (Internet-of-Things Penetration Testing)** and **FOR572 (Advanced Network Forensics)** training to the curriculum. "*The expansion reflects the Galician government's commitment to cybersecurity training,*" Vázquez notes. "*They launched a new project and decided to include additional SANS courses and GIAC certifications after seeing how valuable these are for Galician professionals.*"

The course selection process mirrors the original approach, involving extensive consultation with cybersecurity stakeholders across the region. "*Amtega speaks with all the public and private agents to decide what are the courses that make the difference for the professionals,*" he notes. This collaborative approach ensures training remains aligned with actual market needs.

Spain's autonomous regions operate independently in terms of budget allocation and policy decisions, making Galicia's approach particularly significant as a potential model for other regions. The Spanish government has announced a €1.1 billion investment[2] to enhance cybersecurity, focused on protecting critical infrastructure and improving resilience. Additionally, billions of euros have been earmarked for telecommunications and cybersecurity capabilities through various national plans.

> *"It is about return on investment. SANS training has a high cost, but it delivers an excellent return by enhancing the qualifications of the professionals who complete it."*

CNTG's programme demonstrates how regional governments can contribute meaningfully to national cybersecurity objectives while building local competitive advantage. "*For CNTG, cybersecurity is an important element in the training of IT. In fact, at this moment, it is the most important element of the training centre,*" Vázquez emphasises. SANS has become integral to this strategy: "*They are an excellent provider of cybersecurity training.*"

For other regional governments considering similar investments, Vázquez offers practical advice: "*It is about return on investment. SANS training has a high cost, but it delivers an excellent return by enhancing the qualifications of the professionals who complete it.*" He frames it as a strategic necessity: "*I would simply say that this is training that other entities should invest in because it establishes a differential element for their citizens or professionals. For us, it is a safe bet, a safe investment.*"

[2] https://digital.gob.es/en/comunicacion/notas-prensa/mtdfp/2025/05/2025-05-06_02

Strategic Investments

Galicia's approach to public cybersecurity training offers a blueprint for how regional governments can build cyber resilience through strategic workforce development. The success metrics speak for themselves: high participant satisfaction, measurable professional advancement, increased regional competitiveness, and growing demand that will lead to expanding the programme. More importantly, the programme has created a sustainable model where public investment in cybersecurity training generates returns across the entire regional economy.

For cybersecurity leaders considering similar public-private partnerships, Galicia's experience demonstrates that strategic investments in workforce development can address immediate skills shortages while simultaneously building long-term regional cyber resilience. In an increasingly connected world, where cyber threats know no boundaries, these collaborative approaches may well represent the future of effective cybersecurity defence.

SANS Training at CNTG

SEC504: Hacker Tools, Techniques, and Incident Handling) | GCIH

FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics | GCFA

SEC556: IoT Penetration Testing

FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response | GNFA

SANS Institute

The most trusted source for cybersecurity training, certifications, degrees and research.

Contact Us

+44 203 384 3470

www.sans.org

emea@sans.org

@sansemea

CENTRO DE NOVAS TECNOLOXÍAS DE GALICIA

SANS