

LAC4 Cybersecurity Expert Visit to Guatemala with focus on cyber governance

17-20 September 2024

26 November 2024, EU CyberNet, Contact: Merili Soosalu (merili.soosalu@ria.ee)

The 4-day mission to Guatemala celebrated Guatemala's accession to LAC4 Centre and included four different seminars on cybersecurity governance to the public, private and civil sector that brought together 292 people and were co-organised by the Delegation of European Union to Guatemala (EUD), Presidential Commission for Open and Electronic Government of Guatemala (GAE). Expert team also took part in the National Committee of Cybersecurity meeting.

LAC4 expert team was composed of LAC4 Programme lead, Merili Soosalu and cyber governance experts from Estonia, Kadri Kaska and from Costa Rica, Jorge Mora.

Discussions with Guatemalan stakeholders throughout the week-long consultations indicated that, although some foundational national cybersecurity governance elements are established in Guatemala, there remain considerable gaps that require attention, particularly in the areas of clarity regarding institutional roles and responsibility, legal frameworks, and stakeholder engagement.

The findings from the consultations are organised below according to three central themes: **governance framework, preparedness and response, and cybersecurity awareness and talent**. Each delineates existing resources, identified gaps, priority objectives and actions, and potential partners to accomplish these objectives, as identified by stakeholders during the week's events.

Governance framework

Institutional architecture

There are various structural assets indicating that **a basic institutional architecture exists for cybersecurity capacity and coordination in Guatemala**. This includes the Presidential Commission for Open and Electronic Government (GAE), (National Committee of cybersecurity (CONCIBER), and the Armed Forces' Informatic Command (transitioning to a brigade status). Other key institutional players include the Ministry of the Interior, the Cybercrime Unit, the Ministry of Telecommunications, and the Ministry of Defence's Cyber Defence sector.

Efforts like CONCIBER, Digital transformation coordination (*mesa de transformacion digital*) and GAE's collaboration reflect steps taken to establish **a framework for coordination and planning**.

However, the system as a whole lacks coherence and clear governance, and significant challenges remain. There is confusion about **who is responsible for what in cybersecurity governance**. Key ministries **lack dedicated cybersecurity departments or staff**, making it difficult to drive policy implementation and ensure accountability. There is only minimal collaboration between the Ministries of Defence, Science and Technology, and the broader executive branch, including local governments. The need to establish greater cooperation across government institutions was highlighted as a priority to streamline efforts, improve governance, and facilitate knowledge-sharing.

Furthermore, stakeholders see the Congress of the Republic and local governments as key players with regard to any cybersecurity governance reforms, but they are currently underrepresented in these discussions. Congress, in particular, must play a more active role in advancing the necessary legal framework.

It was also noted that the judiciary needs to be integrated into cybersecurity efforts, with specialised training for judges and prosecutors.

Legal and policy frameworks

An important task to be carried out is the review of the regulatory framework in order to determine short, medium, and long-term actions that can help strengthen the country's cybersecurity governance evolutionarily.

Guatemala has a **National Cybersecurity Strategy** from 2018, but its implementation and effectiveness are uncertain.

The Constitution provides a foundational legal framework, and some **cybersecurity-related laws** were mentioned, though their practical utility was questioned. A **draft bill** is reportedly under development; however, it appears to overlook key issues and is mostly concentrating on cybercrime, thus requiring revisions before it can effectively address the country's cybersecurity needs.

Updating or creating new laws, including data protection and cybersecurity legislation, is seen as the most urgent task by the community. While a revised cybersecurity strategy might need to precede legislative changes, legal reforms remain an issue that local stakeholders perceive as critical and hence it must be addressed carefully. These reforms should clearly

define governance roles, responsibilities, and structures, particularly in areas such as incident management and emergency response. Additionally, several participants highlighted revising the civil service law as essential to allow for the creation of cybersecurity roles and make positions more accessible to a wider group, including young professionals.

Joining **international agreements** like the Budapest Convention was also highlighted as a priority. Although this falls outside of the scope of the LAC4 work, there might be space to support these efforts under other initiatives, such as the GLACY-e (Global Action on Cybercrime Extended), joint EU-Council of Europe project.

Stakeholder cooperation and public engagement

Though limited, early stages of **stakeholder cooperation across sectors** seems to have begun. Social media and other technologies are being used for public engagement and situational awareness, though the efforts are ad hoc and unstructured to date.

There is desire for collaboration between the **private sector and government institutions** for sharing resources and expertise, although current efforts appear very limited. Participants noted collaboration with civil society, the private sector, and local media as a potential venue to enhance public awareness and education around cybersecurity risks.

Civil society is seen as an important partner, particularly in ensuring indigenous communities are included in cybersecurity initiatives, given Guatemala's linguistic diversity.

Universities, through postgraduate programmes, are identified as key contributors to developing a skilled cybersecurity workforce, while academic institutions and think tanks also provide research and training aligned with national needs.

Collaboration with international entities such as the EU, USA's Southern Command (Comando Sur), and regional alliances like LAC4 are known and recognized among stakeholders as useful venues for enhancing knowledge-sharing, capacity-building, and alignment with global cybersecurity standards.

Preparedness and response

The challenges highlighted here fall into three broad categories: (i) technology gaps and insufficient investment; (ii) lack of cybersecurity baseline requirements; and (iii) incident preparedness and emergency response plans.

Insufficient investment and underdeveloped infrastructure pose several challenges to cybersecurity preparedness in Guatemala. The overall low level of investment hampers

building and sustaining robust defences. There is a scarcity of adequate technological tools, and insufficient training for their use. Defence representatives noted that procurement and budgetary constraints prevent the establishment of a Security Operations Center (SOC) for the Armed Forces, while other sectors still lack even more basic cybersecurity tools. The lack of R&D investment was noted as stifling innovation and long-term growth in cybersecurity capabilities.

There are no comprehensive incident response plans in place, response and crisis governance roles are unclear, and institutions lack trained personnel (including in law enforcement and judiciary) to handle cyber incidents.

In terms of **priorities**, ensuring proper licensing for cybersecurity software and tools is a recognised necessity to support operations. Clear government-wide minimum cybersecurity standards and baseline cybersecurity preparedness requirements for both public and private sectors are needed, along with business continuity and disaster recovery plans to ensure that institutions can maintain operations in case of a cyber incident. Establishing a National SOC for coordinated monitoring and response was also mentioned.

In terms of institutional preparedness, establishing clear governance for incident response, including well-defined points of contact (POCs) and communication protocols, is a key priority. Regular cybersecurity exercises, both at the national and international level, are also essential for improving readiness and ensuring that institutions and personnel are capable of responding effectively to cyberattacks.

Cybersecurity awareness and talent

Cybersecurity Awareness

Public awareness of cybersecurity is limited, especially considering Guatemala's linguistic diversity, where 22 languages are spoken beyond Spanish, which complicates effective communication and education around cybersecurity risks and best practices. There is a need for multilingual outreach and communication campaigns to ensure that cybersecurity education reaches all segments of the population.

Stakeholders identified public awareness as a key focus area, noting the importance of raising awareness not only to improve general cybersecurity knowledge but also to prepare the public to address cyber risks. There is also an evident need for leadership buy-in, with targeted awareness campaigns aimed at decision-makers to shift their perception of 'cybersecurity as a cost' to one where cybersecurity is seen as a necessary investment.

Cybersecurity Workforce

There are both **structural and cultural barriers** that hamper the development of a skilled cybersecurity workforce. Outdated civil service laws prevent the creation of new cybersecurity roles within the public sector, further compounded by a lack of dedicated organisational structures. There is a significant shortage of trained cybersecurity professionals, including judges, prosecutors, and technical personnel.

Resistance to basic cybersecurity measures, such as two-factor authentication, in the public sector stems from a broader cultural reluctance to change. This highlights the need for efforts to build a capable workforce to go hand-in-hand with more significant societal shift towards recognising the importance of cybersecurity.

Priorities in this area include reforming civil service laws to create flexible and accessible cybersecurity roles and expanding training to develop a more technically skilled workforce. Raising awareness at all levels, from early education to leadership, will be crucial in addressing both the workforce shortages and the cultural barriers that currently limit Guatemala's cybersecurity capabilities.

Proposed action plan for Guatemala

Based on the conclusions of past mission and continuous discussions with Guatemala, following cyber capacity building activities are proposed to Guatemala by the LAC4 centre of the upcoming year of 2025:

- Inclusion of Guatemala to all LAC4 member countries activities (mostly online trainings) – ongoing;
- Regulatory support to Guatemala cyber laws, strategies – depending on Guatemala's political agenda;
- Train the trainer programme on cyber awareness raising with focus groups on public sector employees and civil society - I semester 2025;
- Launch of EU CyberNet cyber hygiene platform to provide basic-level cyber hygiene course for public officials (<https://www.eucybernet.eu/portfolio/cyber-hygiene-platform/>) - I semester 2025;
- Information Security training for government CISOs – I semester 2025;
- Critical Information infrastructure protection introductory course for government – II semester 2025;
- Small and medium enterprises cybersecurity standards workshop for Central-American countries in cooperation with the EU Delegation of Central-America – 20-22 March 2025 (Antigua);
- Cyber diplomacy seminar for diplomats of Ministry of Foreign Affairs – III semester 2025;
- Possible study visit to Estonia on cyber governance structure and cyber eco-system of Central-American countries (tbc) – III semester 2025

Additional requests by Guatemalan authorities will be considered by the LAC4 project team.