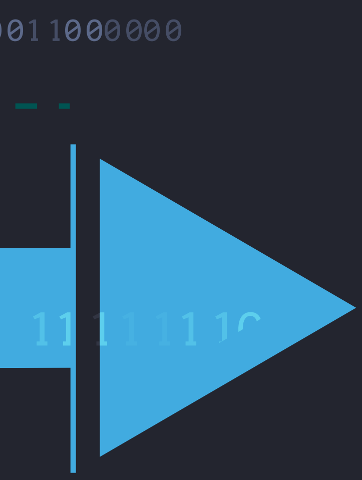
THE BEST PATH FORWARD

How to Effectively Develop a Regional Cyber Security Workforce

By **Pedro Janices**, academic coordinator for the CAPA 8 Foundation; **Mariana Galan**, legal advisor to the Directorate of Cybercrime of the Ministry of Security of Argentina and member of the Commission on Public Policies, Human Rights and Digital Privacy for the CAPA 8 Foundation; **Maximiliano Scarimbolo**, principal officer for the Buenos Aires City Police; and **Agustin Malpede**, lawyer specializing in information law at the University of Buenos Aires

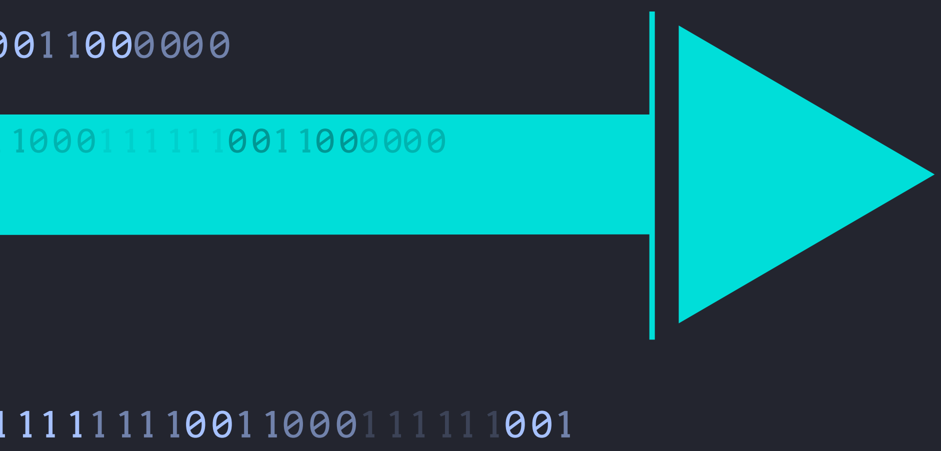
PHOTOS BY NICOLAS LOPE DE BARRIOS

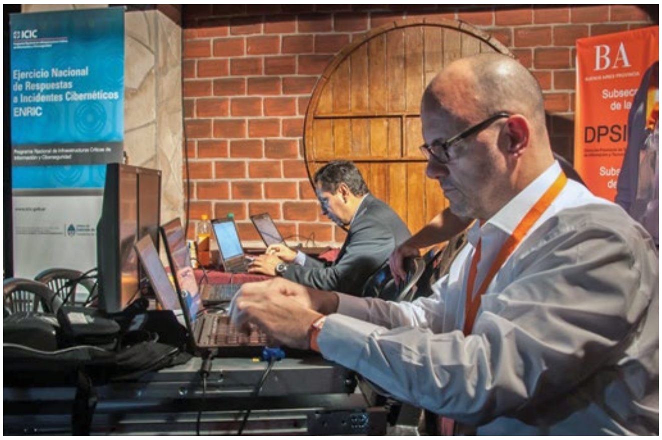


The outbreak of COVID-19 in early 2020 created an urgent need for some countries to adopt social isolation measures and to encourage teleworking, forcing companies and governments to use all the digital tools at their disposal and to increase their availability and access. Organizations that had little or no digital infrastructure were forced to acquire and deploy new digital resources in a very short time, learning as they went.

The pandemic has resulted in a state of increased hyperconnectivity. This is due to a number of factors, such as business and service continuity and an increase in leisure time and digital relationships, forcing people into information self-overloads and making apparent the need for multidisciplinary cyber security teams that focus on crime and safety.

The situation has also brought to light the importance of critical information infrastructure, showing that cyber security not only affects states and the private sector, but also everyone who maintains, contributes to and uses networks. This demonstrates the urgent need to work toward the development of a cyber security workforce that allows nations to take progressive action by training personnel, promoting cyber security awareness in society, passing necessary laws to build a solid legal framework and proposing new public policies in cyber security-related matters. This is not an easy task since it requires the collaboration of every actor involved, each in one's own place, to secure what is necessary to collaborate in the development of a cyber security workforce.




Ejercicio Nacional de Respuestas a Incidentes Cibernéticos ENRIC
BA
DPSI

While some countries in Latin America and the Caribbean have shown interest and commitment to training and exercising to develop further capacities, much still needs to be done to consolidate an ecosystem among the various sectors that allows taking the necessary actions on a regional basis.

From a cultural and social point of view, the development of a regional cyber security workforce should include values, practices and attitudes, and the habits of individual users, experts and other actors in the cyber security ecosystem. The cultural and social perspective varies according to the roles and functions of the actors within this ecosystem. Economic factors also significantly influence whether cyber security measures are efficient.

Law enforcement agencies throughout the region are fully involved in the investigation of cross-border crimes, collaborating with their regional and international counterparts.

LAW ENFORCEMENT

In the field of law enforcement, officers receive constant training in cyber security, although most of them are explicitly focused on cyber crime and cyber terrorism. These activities involve both governmental and nongovernmental organizations (NGOs), which provide a wide range of instructors from Latin America and other regions of the world.

Law enforcement agencies throughout the region are fully involved in the investigation of cross-border crimes, collaborating with their regional and international counterparts. However, in a number of Latin American countries, due to their investigative systems, law enforcement agencies do not have the comprehensive institutional capacity required to investigate and handle cyber crime-related cases and other digital felonies. In these countries, this is the prerogative of the judiciary system, which often leads to bureaucratization and slow investigations.

Informal training, meetings and workshops have proven useful when promoting regional integration and cooperation among numerous agencies, helping to create nonofficial networks of contacts and cooperation channels. Law enforcement now needs to formalize these networks of contacts and links and advance to a more planned and professional system of training.

Law enforcement agencies must monitor and assist this progressive professionalization process wisely, creating technical and operative multiagency protocols and providing the necessary training at each level, which will raise standards and empower the cyber security workforce.

Significantly, establishing regional training and capacity building integration between law enforcement agencies would generate a solid workforce that can face the global challenges of cyberspace.

Argentina, for example, conducted the National Cyber Incident Response Exercise between 2011 and 2015, training a 30-member task force, integrated with members of federal law enforcement forces (Federal Police, Coast Guard, Gendarmerie and Airport Security Police), the Armed Forces, lawyers, prosecutors, judges, technical teams from companies and members of government agencies. These exercises, which began under the auspices of the Organization of American States (OAS) Inter-American Committee Against Terrorism, gave impetus to the need for joint work and the development of specific capacities respective of local laws and culture. Despite these constructive efforts, Argentina's change of government brought in an administration with a different philosophy regarding the exercises, which were discontinued in 2016.

Participants at the National Cyber Incident Response Exercise, May 14, 2015, Mar del Plata city, Buenos Aires, Argentina

PRIVATE SECTOR

Despite efforts being made, Latin America still finds itself in a situation of urgent need. According to the "Cybersecurity Report 2018-2019" from VU Labs, a company that focuses on fraud prevention and identity protection, 45.3% of participating organizations from different countries were victims of a cyber attack during the past three years. In the same vein, according to the "2018 Internet Security Threat Report" by Symantec, Argentina occupies eighth place as the country of origin for cyber attacks. Although the 2016 cyber security report from the OAS and the Inter-American Development Bank (IDB), "Cybersecurity: Are We Ready in Latin America and the Caribbean?" indicates that the region is accelerating development in cyber security matters, regional capabilities are still limited compared to our European counterparts.

In Latin America, the local branches of multinational corporations do not strive to raise cyber security awareness, as do their head offices. As a result, they fail to develop an adequate cyber security workforce that allows them to face the many challenges that cyberspace presents. Here, the academic sector will play a fundamental role. At this time, cyber security-related topics can only (and hardly) be found in university careers or postgraduate courses, severely limiting the possibilities for developing a strong, cyber-resilient and cyber-aware workforce.

To overcome these obstacles, Latin American countries need to set clear and transparent rules and lay the foundation for a solid legal framework, taking actions such as:

- Supporting and developing national cyber industries that are best suited to understanding local culture and identifying the cyber security needs of each country in the region. This is done, for example, by creating effective tax incentives for actors who invest in and promote the evolution of information and communication technologies (ICT).
- Strengthening public-private cooperation involving national and international ICT companies, as well as the academic sector and civil society. This would close the gap between sectors and generate a wide, integral vision of the current state in the region.
- Developing societal trust in national digital infrastructure, promoting collaboration in every sector and allowing each citizen to be involved in the decision-making process.
- Enhancing traditional education tools at every academic level, helping citizens to adopt new habits with full knowledge of the risks that cyberspace represents.

Raising the maturity level of subsidiaries of multinational companies in the region will allow, among other benefits, the adoption of safety standards for this sector, the defining of security policies and the implementation of new methodologies. It will raise awareness of the security risks and the training of human resources from a security point of view, generating opportunities to share knowledge and experiences. The private sector must understand the need to use standards developed specifically to deal with cyber security-related matters and comply with the necessary legal framework accompanying the process.

PUBLIC SECTOR

The region's public sector awareness of the importance of developing cyber security strategies and regulatory frameworks has increased in recent years, reaching a medium level of commitment as indicated by the "Global Cybersecurity Index 2018" from the United Nations' International Telecommunications Union.

While some Latin American countries are in the process of developing their own strategies, others, such as Argentina, Chile, Colombia,

National Cyber Incident Response Exercise, May 20, 2014, Puerto de Buenos Aires, Argentina

Mexico, Paraguay and Peru, already have theirs in play. This fundamental pillar must be considered when trying to generate long-term public policies and regulatory frameworks. The maturity level of these strategies varies, including in terms of providing a framework for cooperation between government agencies, critical infrastructure operators and the private sector.

Latin American countries have different approaches, priorities and attitudes regarding the development of a cyber security workforce. While the public sector recognizes the need to work on topics that range from internet governance and innovation, to providing public services and the acquisition of digital equipment, there is still a medium/low level (50% average) for internet penetration in the region.

Social and economic problems play major roles in defining each country's vision regarding the development of its workforce. For example, some will have a more privacy-oriented vision and others may choose a military approach to the subject.

The development of a solid legal framework, new standards and technical regulations is moving slowly in the region. As mentioned before, only a few Latin American countries have implemented their own cyber security strategies and even fewer consider it a necessary state policy, update their digital infrastructure or focus on capacity building.

International organizations such as the OAS or the IDB provide constant support in raising cyber security awareness and capacity building. They also encourage countries to join different international initiatives such as the Global Forum on Cyber Expertise and the Internet Governance Forum.

Some Latin American citizens don't fully understand the risks and vulnerabilities that ICTs present. This has led countries from the region to make efforts toward sensitizing and training human resources, which will continue over time, and even to associate with international campaigns, aiming for a cyber-resilient and cyber-aware society.

In the case of a cyber incident, the amount of information passed through formal channels is rather low. On the other hand, much more information flows through informal channels. Formal channels seem to be severely affected by factors such as the fear of filing a formal complaint, poor complaint communication mechanisms and by the lack of knowledgeable authorities to receive them, and even by the difficulty of taking not only reactive, but preventive measures.

This is closely linked to the adoption of regulatory frameworks to prevent cyber crime. Most countries in the region understand the transnational nature of these crimes, and cooperation has deepened in recent years. Argentina, Chile, Colombia, Costa Rica, the Dominican Republic, Panama, Paraguay and Peru have now acceded to the international Budapest Convention, a treaty that addresses cyber crime. Work is also under way in a number of intergovernmental bodies on the drafting of new instruments of cooperation in which a larger and more diverse group of countries can discuss criminal conduct and new cooperation mechanisms with an understanding of regional asymmetries. However, the prosecution rate of cases is low, the judiciary does not have sufficient forensic tools for investigations, and training in this area is scarce.

NGOS AND CIVIL SOCIETY

NGOs play a major role in Latin America, especially in Argentina. They contribute to and cooperate in visualizing, understanding and even improving public policymaking. This is why it is vital to take into consideration the opinion of every actor involved and promote the development of a solid legal framework that focuses on privacy, human rights, and capacity building of technical and legal resources.

NGOs are also an important source for free debate, speech and thought, which will considerably benefit the strength and resilience of regulations applied in each state. Accordingly, a United Nations resolution (A/RES/73/27), passed on December 5, 2018, endorses this type of government support: "States should encourage the private sector and civil society to play an appropriate role to improve security of and in the use of ICTs, including supply chain security for ICT products and services. States should cooperate with the private sector and the organizations of civil society in the sphere of implementation of rules of responsible behavior in information space with regard to their potential role."

Clear examples of this are the workshops and congresses where Fundación CAPA 8, an Argentina-based nonprofit that studies and advocates for cyber initiatives from a human rights perspective, gathered representatives from the executive, legislative and judicial powers, as well as law enforcement and the armed forces. The private sector, academy and press were also present and contributed with their knowledge and viewpoints, generating a healthy debate about the successes, errors and challenges that Argentina faces in its fight against cyber crime.

CONCLUSION

The Global Information Security Workforce study, conducted by the Center for Cybersecurity and Education in 2017 in 170 countries, reveals that there will be a cyber security manpower shortage of more than 1.8 million workers by 2022 and concluded that there are not enough cyber security workers in organizations to address the challenges they face today.

Workforces that focus on protecting a country's cyberspace require expertise and both initial and continuing professional training to be able to respond adequately to the scale and evolution of cyber incidents. Generating the necessary training from the law enforcement training institutes (Federal Police, Coast Guard, Gendarmerie and Airport Security Police) would require at least two years of instruction.

For this, it is necessary to promote state policies on cyber issues, sustained over time through the essential contributions of the different actors in the cyber ecosystem: the public and private sectors, academia and NGOs.

The "new normal" will find us with hyper-connected governments, companies and citizens, and we will have to respond to threats with specialized technical, legal and diplomatic teams.

Cooperation and collaboration between countries ceases to be mere diplomacy and becomes a case of cyber survival for all and working toward regional resilience. To this date, progress in Latin America, in most cases, has been the result of efforts that have also highlighted the weaknesses of those countries in the region that have not yet begun the journey.

The "new normal" will find us with hyper-connected governments, companies and citizens, and we will have to respond to threats with specialized technical, legal and diplomatic teams. Will we be on time? Will we come to equalize the regional asymmetries? The challenge is ours. □