2023

Report on
CYBERSECURITY WORKFORCE DEVELOPMENT
in an Era of Talent and Skills Shortages

OAS More rights for more people

Cybersecurity Innovation Councils

CISCO

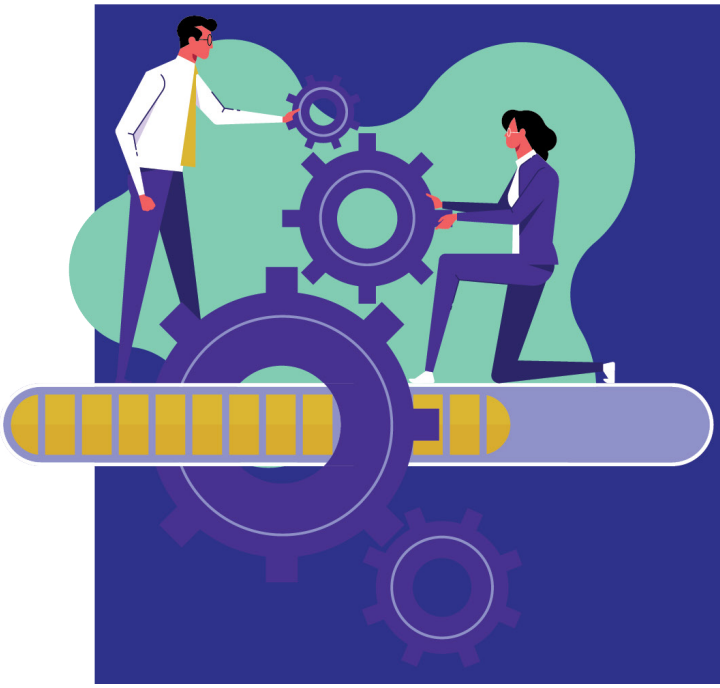
Prepared and published by the Cybersecurity Program of the Inter-American Committee against Terrorism (cybersecurity@oas.org)

EXECUTIVE SUMMARY

The COVID-19 pandemic and post-pandemic era have had major impacts on the global economy,[1] given rise to an expanded threat and risk landscape,[2] and ushered in a sea change in how organizations work.[3] In addition, we have seen an aging population,[4] serious problems due to high unemployment,[5] and setbacks in progress toward gender parity.[6]

The cybersecurity labor market has faced a gap (shortage) in its workforce in the near term,[7] creating risks due not only to talent shortages in organizations, but also to skills shortages in the workforce. This situation, although global, has been exacerbated in Latin America and the Caribbean, putting tremendous pressure on both public and private organizations, with the subsequent impact on cybersecurity in the region's countries.

Cybersecurity workforce development is currently analyzed under two approaches: quantitative (in the context of the shortage of professionals) and qualitative (in terms of the skills gap of professionals wishing to join the cybersecurity workforce as well as those already in the workforce). Analyzing the situation on both the demand and supply sides of the cybersecurity labor market is crucial to identifying the problems and challenges that all the multiple stakeholders need to address in order to close the gaps in the countries of the region.



For example, on the supply side, for those interested in entering the cybersecurity job market, the information about what a career entails is overwhelming, confusing, and contradictory. The path to be followed to prepare for a cyber career and advancement once in the workforce can be a complex one. On the demand side, organizations face challenges in identifying the requirements needed to fill open positions and to recruit and retain talent while trying to maintain a strong cybersecurity posture. Governments have been adopting and implementing national cybersecurity policies and strategies to address the lack of cybersecurity capabilities; however, the proposed strategic initiatives around cybersecurity workforce development in the region will take years or even decades to mature.

1 After a strong rebound in 2021, the global economy is entering a pronounced slowdown amid new threats of COVID-19 variants and rising inflation, debt, and income inequality that could jeopardize the recovery of emerging and developing economies. Growth in Latin America and the Caribbean is projected to slow to 2.6% in 2022 before rising slightly to 2.7% in 2023 (WORLD BANK, 2022).
2 The Latin America and Caribbean region was hit by 137 billion attempted cyberattacks from January to June 2022, an increase of 50% over the same period last year (with 91 billion). Mexico was the most attacked country (with 85 billion), followed by Brazil (with 31.5 billion), and Colombia (with 6.3 billion) (FORTINET, 2022).
3 According to Forbes (FORBES, 2022), the future of work will be more hybrid, more collaborative, and more automated.
4 Over the next fifty years, the elderly are expected to outnumber the young in almost every country. This demographic shift has enormous implications for all aspects of society and the economy (Oxford Martin School, 2022).
5 Global youth unemployment is expected to reach 73 million in 2022, a slight improvement over 2021 (75 million), but still six million above the pre-pandemic level of 2019 (ILO, 2022).
6 According to the World Economic Forum (WEF, 2022), it will take another 132 years to close the global gender gap.
7 There is a global shortage of 3.43 million skilled cybersecurity workers (ISC2, 2022a).

Cybersecurity workforce development is vitally important to national preparedness for conflicts in cyberspace. It is also crucial to helping organizations define the skills and capabilities needed in their workforce to meet their strategy and business objectives, identify key gaps in the current workforce, and create innovative strategies and programs to attract, recruit, hire, and develop the best talent.

The cybersecurity workforce and skills shortage will continue to grow in Latin America and the Caribbean. Therefore, the cybersecurity ecosystem in the region must take a comprehensive and coordinated approach to workforce development in order to address a unique combination of problems and challenges, all while moving from problem-solving to action.

CREDITS

Luis Almagro
Secretary General
Organization of American States

Luis Oliveira
Secretary for Multidimensional Security
Organization of American States

Alison August Treppel
Executive Secretary
Inter-American Committee against Terrorism
Organization of American States

OAS Technical Team
Kerry-Ann Barrett
Orlando Garcés
David Moreno
Mariana Cardona

CISCO Technical Team
Rebeca De La Vega
Mario De La Cruz
Ned Cabot
Frederico Vasconcelos
Vinita Venugopal

TABLE OF CONTENTS

CHARTS

TABLES

01

INTRODUCTION

Latin America and the Caribbean remain committed to maximizing the benefits provided by Information and Communication Technologies (ICT), because they are powerful tools that help transform the lives of every citizen. The creation of more and better infrastructure to deliver internet access has a direct impact on the economic and social development of the region. Hence, the countries of the region must increase digital trust.

Due to the sharp increase in cyber threats, efforts to improve cybersecurity capabilities have grown substantially in the region. However, one area that continues to lag behind is cybersecurity workforce development. There is a shortage of trained and qualified personnel in the labor market to work in cybersecurity roles that can address these threats and their associated risks.

Cybersecurity skills can be acquired, changed, and enhanced through **education, training, or apprenticeships,** making the cybersecurity workforce an evolving talent pool that public and private organizations in the region should develop and maintain.

The shortage of cybersecurity professionals and skills is a multidimensional policy issue involving multiple stakeholders (public sector, private sector, academia, and civil society) and is exacerbated by many factors. Avoiding the challenges related to this shortage would create problems for both the economic development and national security of countries in the Latin America and the Caribbean region.

This report presents a **detailed analysis of the cybersecurity labor market and workforce in the region** in the current cybersecurity environment, identifying issues and challenges that need to be addressed comprehensively by multiple stakeholders, in line with international best practices. The research involved a review of academic and grey literature, as well as other material produced by governments and organizations to gain insight into the professional and skills gap in the cybersecurity workforce.

This report is divided into five chapters, this being the first chapter. The second chapter outlines the existing cybersecurity landscape and identifies factors influencing the cybersecurity labor market and workforce. The third chapter describes this labor market and the conditions that affect it on both the supply side and the demand side, characterizing the current labor force. It also describes the main problem and identifies a unique combination of challenges facing the market today. A proposed solution for multi-stakeholder action to promote workforce development and solve the identified problem is presented in the fourth chapter. Finally, the fifth chapter presents the bibliographic references consulted for this research.

02

CYBERSECURITY IN TODAY'S CONTEXT

The development of a digital economy contributes positively to economic and social prosperity in the countries of the Latin America and the Caribbean region. This requires building a secure and reliable digital environment to accommodate the proliferation of the digital activities of governments, organizations, and citizens. Many of the challenges facing the digital economy today are due in large part to dependence on the internet and its rapid growth in terms of both users and applications.

This situation demands that the region have sufficient capacities for the appropriate and timely management of inherent cybersecurity risks, so that, although increased use of the digital environment increases exposure to risks, the actions taken will reduce digital incidents to prevent economic or social consequences derived from threats, attacks, and cyber incidents that erode digital trust and hinder adaptation to the digital future. By responding appropriately to today's cybersecurity challenges, the digital transformation can be fully leveraged and individuals, organizations, and society as a whole can capitalize on new opportunities.

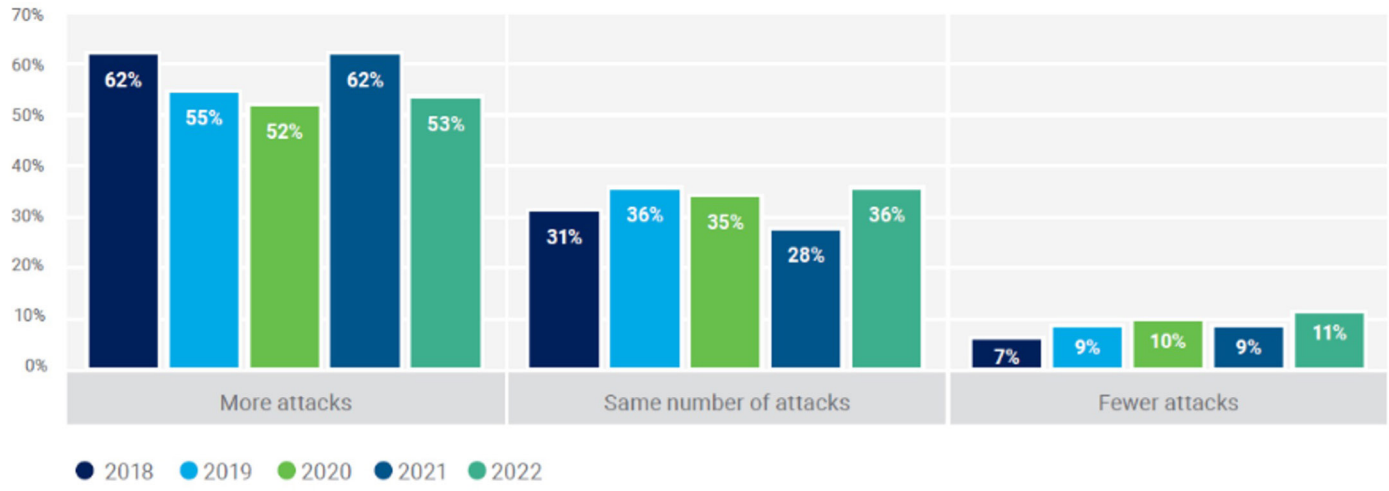
The COVID-19 pandemic has created a complex economic situation in Latin America and the Caribbean over the past three years. Restrictions and other public health interventions implemented to reduce the spread of infection have had a major impact on the region's economy. Organizations and citizens migrated en masse to digital and online channels to circumvent social distancing measures, continue business operations, secure revenue streams, and remain solvent during the pandemic (IDB, ECLAC & KAS, 2021). However, some economic sectors such as the ICT sector saw not only increases in hours worked but also growth in employment compared to the years preceding the pandemic (OECD, 2021).

Organizations, especially SMEs[8] in the region, faced hasty digitalization and digital transformation processes. However, the lack of digital skills has become a cross-cutting challenge for this business segment and has emerged as a key obstacle in addressing these processes. Many organizations lack a digital culture at both the strategic and operational levels where the potential benefits of digitalization are often unknown or not fully understood.

8 SMEs make up 99.5% of businesses in the Latin America and Caribbean region (with nearly 9 out of 10 classified as microenterprises) and generate 60% of formal productive employment. However, Latin American SMEs have a particularly significant productivity gap, accounting for only a quarter of the region's total output value (OECD, 2022).

There is a growing expansion of the threat and risk landscape globally and in the Latin America and Caribbean region. As dependence on digital technologies continues to rise, so does cybercrime. Cybercriminals are taking every opportunity to exploit vulnerabilities against people and organizations through technology, rapidly adapting new technologies, tailoring their attacks using novel methods, and cooperating closely with each other (WEF, 2022). According to ISACA, during 2018 and 2022, between 52% and 62% of organizations perceived that they sustained more attacks[9] than in the immediately preceding year (ISACA, 2022).

Chart 1.
Year-over-year comparison of cybersecurity attack reports

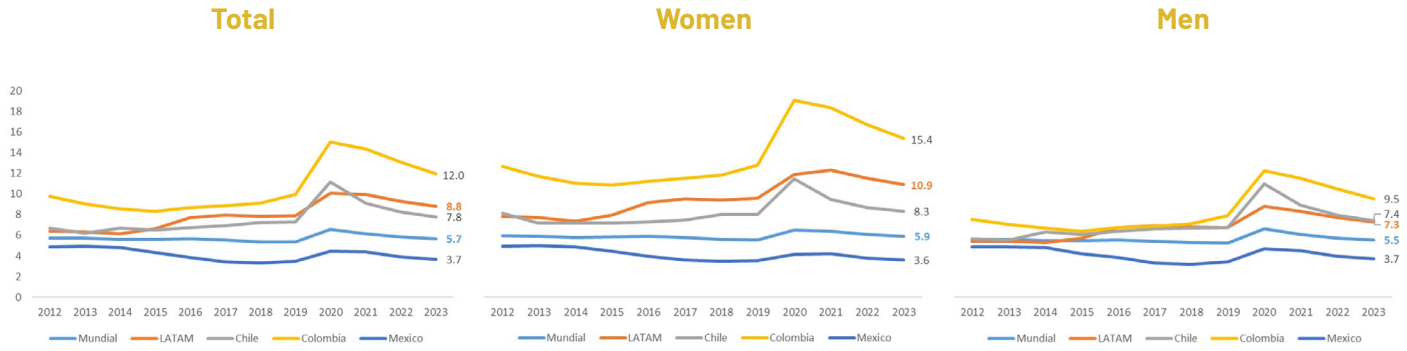


Source: (ISACA, 2022).

Labor markets are undergoing a period of profound transformation. Jobs and skills have been affected by automation,[10] the transformation of industry, and the ecological transition, coinciding with pandemic-driven changes in labor practices that had seemed impossible before.[11] In particular, the role of technology has grown exponentially in all sectors of the economy, creating new occupations and altering the tasks performed by humans and the skills they need to make their way in the labor market (IDB, 2021). However, technology can generate technological unemployment and increase both inequality and polarization in the region if governments, organizations, and individuals do not respond appropriately (IDB, 2020).

9 Ransomware, social engineering, and malicious insider activity are the top three cyberattacks that organizations are most concerned about, while infrastructure failures due to cyberattack, identity theft, and ransomware are the top three cyberattacks that most concern cyber leaders (WEF, 2022).
10 Nearly half (48%) of World Economic Forum Cyber Outlook respondents say automation and machine learning will usher in the biggest transformation in cybersecurity in the near future (WEF, 2022).
11 https://www.weforum.org/events/world-economic-forum-annual-meeting-2022/sessions/a-new-vision-for-jobs

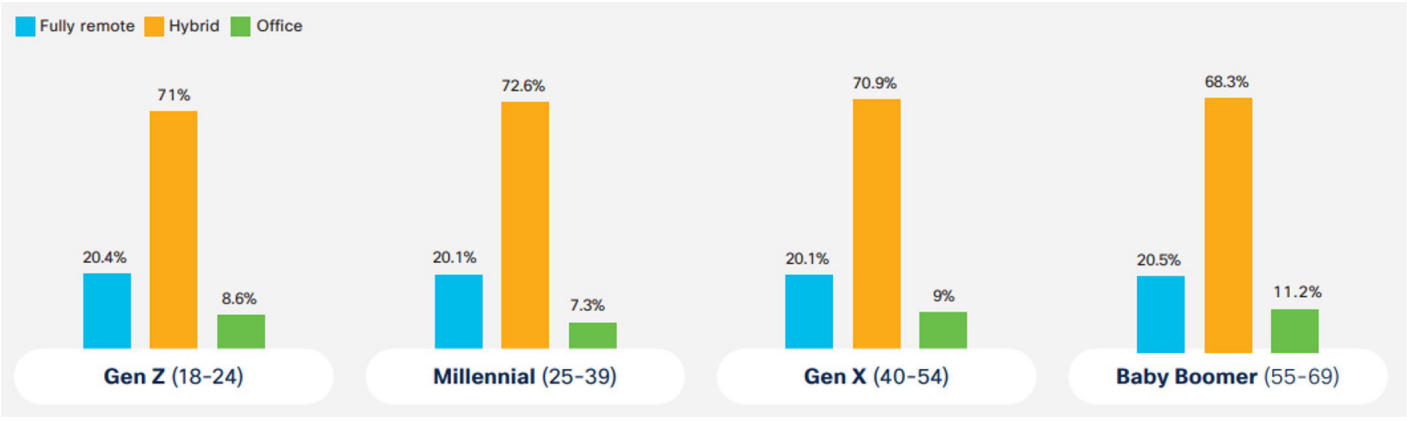
Chart 2.
Evolution and projection of the unemployment rate in Latin America



Source: Prepared by the authors based on ILO data (ILO, 2022)

Important changes have been made in the way organizations in the region work. Fewer than 20% of organizations in Latin America and the Caribbean currently operate exclusively on a work-from-home basis, 37.5% have returned to the in-person model, and 44.3% say that they are working under a hybrid or mixed model (MichaelPage, 2022). According to the World Economic Forum (WEF, 2022), 28% of executives estimate that the remote/hybrid work environment will be one of the biggest influences on cybersecurity transformation in the next two years.

Chart 3.
Workplace preferences by generation

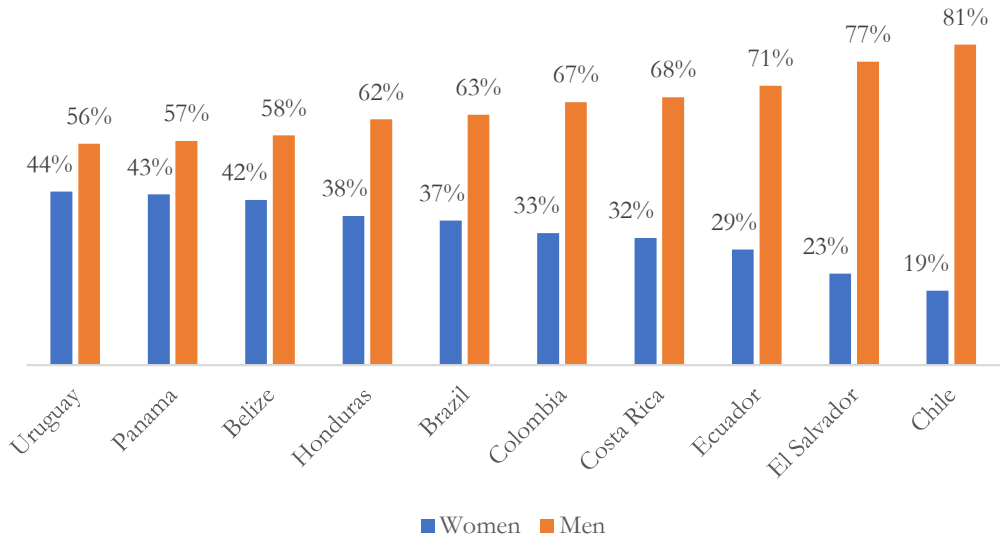


Source: (CISCO, 2022)

Some regions of the world are experiencing phenomena such as *the Great Reshuffle or the Great Resignation,*[12] *or Quiet Quitting.*[13] The departure of many people from their jobs in search of more fulfilling roles with greater flexibility has led to a record number of job openings and staff shortages in some industries.[14] In the wake of this phenomenon, organizations globally are reexamining business strategies, workforce models, values, and culture, often guided by new demands from employees themselves (LinkedIn, 2022).

Progress in gender parity in labor participation has been reversed with significant implications for other dimensions of employment and the distribution of unpaid work, affecting how women access opportunities in the economic sphere, as well as in other spheres of life. The global gender gap as of 2022 has been closed by 68.1%. Another example is that women are underrepresented in STEM-related labor markets,[15] and the gender gap is most prevalent in the ICT sector.[16] Latin America and the Caribbean will close their gender gap in approximately 67 years (WEF, 2022).

Chart 4.
Percentage of male/female graduates of tertiary education STEM programs in Latin America



Source: Prepared by the authors based on information from the Global Gender Gap Report 2022 (WEF, 2022).

12 *The Great Resignation* has certainly sharpened the focus on retention within organizations, which is one of the top requests from CEOs to their HR leaders this year. Interestingly, employees' reasons for staying with their company do not differ much by country and industry, but they do differ by generation. Gen Z employees place more value on inspiring leaders, but not on competitive salaries. For baby boomers, vacation/time off policies are the number two reason they have stayed. Job security is number one across all generational groups in the workforce (MERCER, 2022).
13 During 2022, a new trend has emerged in the labor market called *Quiet Quitting*, which is about rejecting the notion that work has to take over life and that employees must go beyond what their job descriptions entail.
14 https://www.weforum.org/agenda/2022/02/great-reshuffle-jobs-market-resignation/
15 STEM is an acronym for Science, Technology, Engineering, and Mathematics.
16 The percentage of women graduates in ICT at the global level is 1.7%, compared to 8.2% for men (WEF, 2022).

The accelerating pace of digitalization and changing work habits is driving cyber resilience.[17] Executives are planning to improve cyber resilience in their organizations by strengthening resilience policies, processes, and standards on how to engage and manage third parties (WEF, 2022). This is occurring not only in private organizations but also in the public sector.

Against this backdrop, countries in Latin America and the Caribbean have been adopting and implementing national cybersecurity policies and strategies,[18] devising actions to create a more reliable digital environment suitable for achieving their economic and social development objectives. It is therefore particularly important to formulate and implement initiatives that support capacity building for organizations and citizens to manage cybersecurity risks.

In line with best practices,[19] **national policies and strategies in the region address issues related to cybersecurity training and awareness-raising for government entities, citizens, businesses, and other organizations** critical to enabling the digital economy in the region. Good practices include establishing cybersecurity curricula and awareness programs, expanding training curricula and vocational training programs, adopting international certification standards, and fostering innovation and research and development (R&D) clusters. The following are some of the most notable initiatives:

A *Colombia's National Digital Trust and Security Policy (2020-2022),*[20] one of the three specific objectives of which is to strengthen the digital security capabilities of citizens, the public sector, and the private sector in order to build digital trust in the country by formulating strategies and actions for professional training and developing competencies under a differential and inclusive approach.

B *Chile's National Cybersecurity Policy (2017-2022)*[21] sets five objectives, including the development of a cybersecurity culture based on education, good practices, and responsibility in the use of digital technologies through initiatives that promote and develop an aware, competent, informed, and responsible digital culture that includes all relevant stakeholders.

C *Mexico's National Cybersecurity Strategy (2017-2021)*[22] establishes as one of its five cross-cutting axes the development of capabilities through actions aimed at generating and strengthening organizational capabilities, human capital, and technological resources in the area of cybersecurity, which will provide society, academia, the private sector, and public institutions with the resources to manage risks and threats in cyberspace and to enhance national resilience.

17 (WEF, 2022) defines cyber resilience as *"the ability of an organization to transcend (anticipate, withstand, recover from, and adapt to) any stresses, failures, hazards and threats to its cyber resources within the organization and its ecosystem, such that the organization can confidently pursue its mission, enable its culture and maintain its desired way of operating."*

18 Currently, 17 member states of the Organization of American States (OAS) have approved their national cybersecurity policies/strategies (OAS & GPD, 2022), and 14 of them were able to do so with the technical support of the OAS.

19 *The Guide to Developing a National Cybersecurity Strategy* of the International Telecommunication Union (ITU) presents best practices in this area (https://www.itu.int/en/ITU-D/Cybersecurity/Documents/NCS%20Guide_s.pdf)

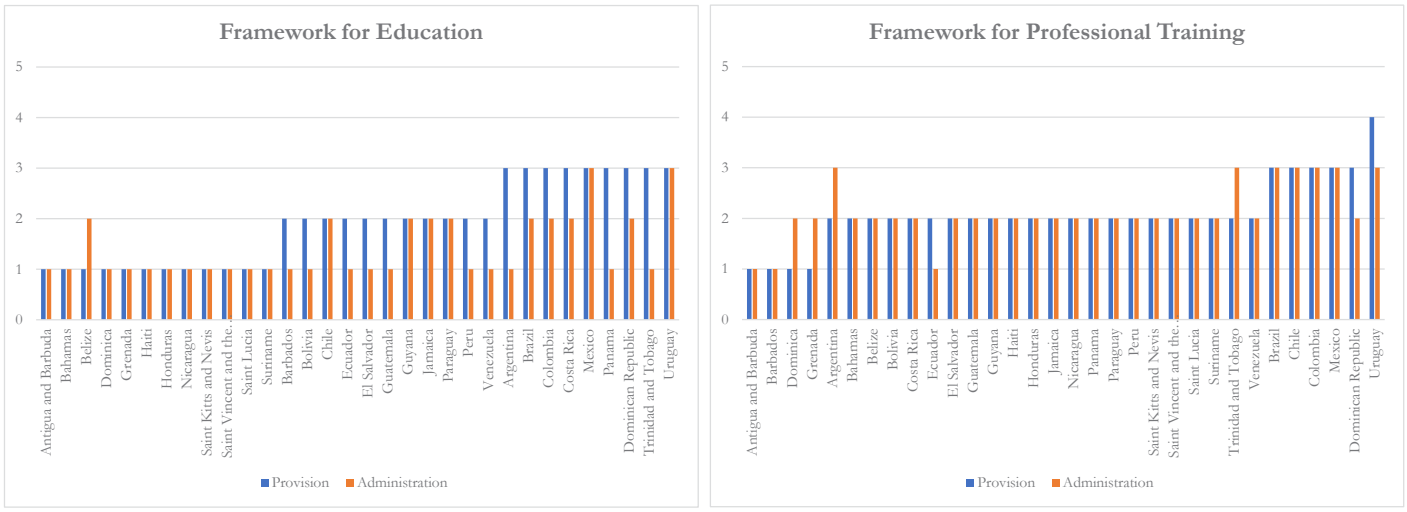
20 Colombia's National Digital Trust and Security Policy was issued through CONPES Document 3995 of 2020 (https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf)

21 https://www.cnc.cl/wp-content/uploads/2020/02/Pol%C3%ADtica-Nacional-Ciberseguridad.pdf

22 https://www.gob.mx/gobmx/documentos/estrategia-nacional-de-ciberseguridad

However, such strategic initiatives related to the cybersecurity labor market will take years or even decades to mature. It takes many years to develop a digitally savvy workforce with skills oriented to a knowledge economy, due to high attrition rates in the public sector for cybersecurity jobs and low rates of availability of cyber-specific educational opportunities (OAS & GPD, 2022). Countries in the region should therefore prioritize workforce development initiatives so they can allocate the budget needed to implement such programs as soon as possible.

Chart 5.
Maturity level of skills in Latin America and the Caribbean in relation to education and professional training



Source: Prepared by the authors based on (OAS & IDB, 2020)

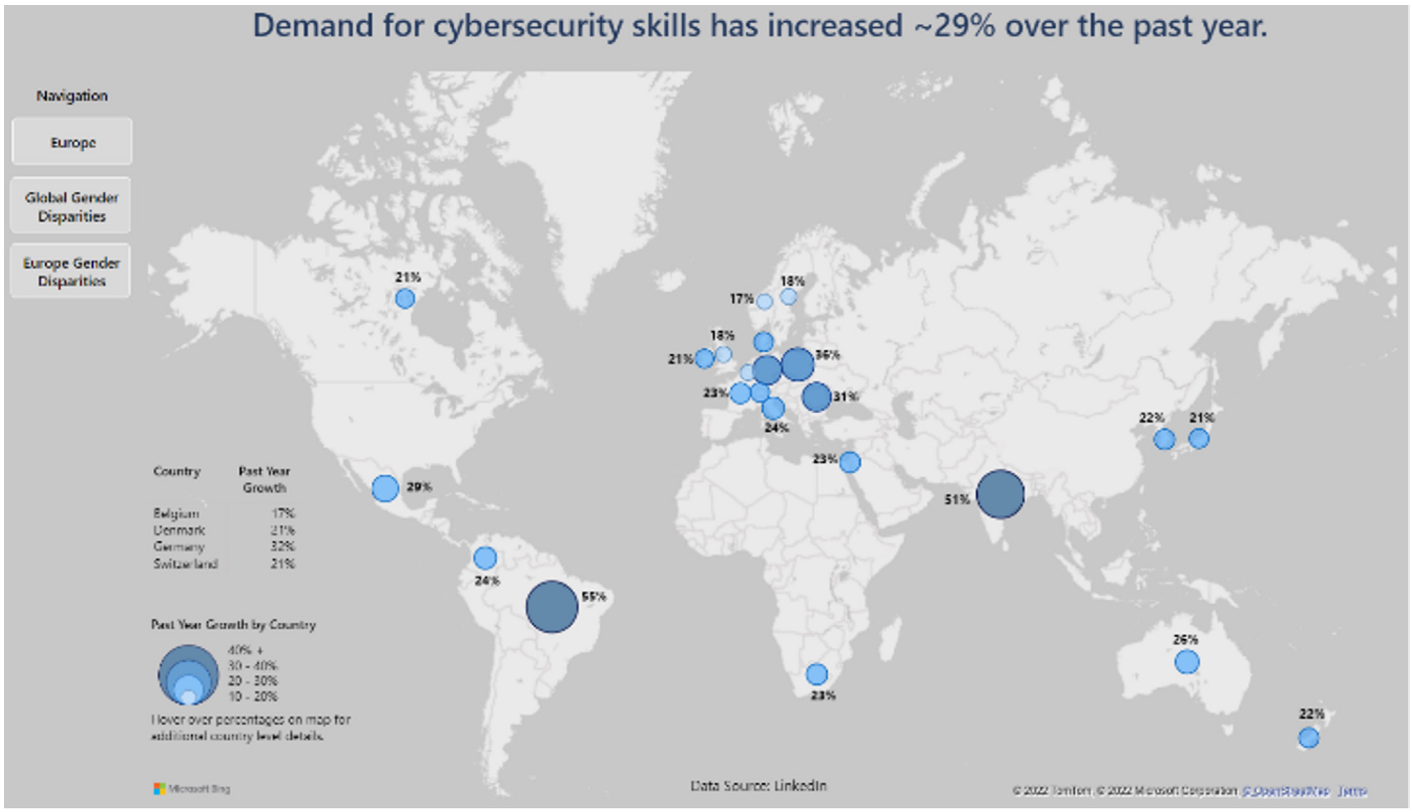
Meanwhile, increased demand for cybersecurity professionals[23] is coupled with a substantial increase in salaries[24] and keen competition among skilled professionals. In this labor market, in the short term, the supply of cybersecurity professionals is not responsive to higher salaries as it takes time to train additional workers with the requisite skills. Training and education efforts can take years; even if individual workers in other occupations, sectors, or industries have the right skill sets to become cybersecurity professionals, they may not change occupations immediately.

23 Increase due to improved connectivity, increased vulnerability, and growth of cybercrime, along with external shocks to the market due to the COVID-19 pandemic.
24 In the UK, employers and cyber teams continue to feel the impact of the pandemic. In particular, it may have led to higher market rate salaries outside London and South East, presenting challenges for smaller, regional employers (DCMS & IPSOS, 2022).

This situation in the region's cybersecurity labor market creates a gap (shortage) in the workforce in the short term. According to ISC[2], there is a shortage of between 515,000 and 701,000 skilled cybersecurity workers in the Latin America and the Caribbean region (ISC2, 2021) (ISC2, 2022a). This study found that the workforce gap remains the top barrier to meeting organizations' security needs, with 60% of respondents reporting that the cybersecurity workforce shortage is putting their organizations at risk.[25]

Risks in organizations are created not only by the shortage of talent but also by the shortage of skills[26] in the workforce. For example, 59% of all respondents to the *Global Cybersecurity Outlook* 2022 study reported that they would find it difficult to respond to a cybersecurity incident in their organizations due to a skills shortage within their team (WEF, 2022).

Chart 6.
Increased demand for cybersecurity skills



Source: (MICROSOFT, 2022)

25 ISC2 confirms, from the global perspective, that when the cybersecurity workforce is small, the negative consequences are real: misconfigured systems, slow patch cycles, rushed implementations, insufficient time for proper risk assessment, insufficient oversight of processes and procedures, and more (ISC2, 2021).
26 According to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework of the National Institute of Standards and Technology (NIST), it is understood that skills represent a combination of abilities, knowledge, and experience that enable an individual to complete a task well in a cybersecurity role in an organization.

This situation has brought intense pressure to bear on both public and private organizations,[27] as they must identify, attract, and recruit the best talent available and retain it by implementing, among others, innovative training and education strategies, such as: (i) *Upskilling* (processes of learning new skills or teaching new skills to employees), (ii) *Reskilling* (processes of training employees in a completely new skill set to prepare them to take on a different role within the company), and (iii) *New Skilling* (continuous learning processes to help develop high-demand skills, whether an individual is trying to improve current capabilities or needs a complete upgrade to develop entirely new ones). It also encourages work-based learning programs, including apprenticeships and traineeships.

These problems in organizations can undermine the cybersecurity of nations and the region. This means that the multiple stakeholders in the cybersecurity ecosystem involved in the development of these labor markets face a unique combination of challenges that Latin American and Caribbean countries must address.

27 Specifically in the UK cyber sector, there is evidence of a more challenging labor market from an employer perspective. More than half of the companies in the cyber sector (53%) have tried to hire someone in the previous 18 months. Of all vacancies during this period, 44% of companies reported that they were difficult to fill (compared to 37% in 2021 and 35% in 2020). The most common reason given for hard-to-fill vacancies continues to be that candidates lack technical skills and knowledge (43% of employers with hard-to-fill vacancies). This year, mentions of competition from other employers have increased (from 9% in 2021 to 25% in 2022), and more people now also cite a general lack of candidates (from 13% to 25%) (DCMS & IPSOS, 2022).

03

THE CYBERSECURITY LABOR MARKET FACES A UNIQUE COMBINATION OF CHALLENGES

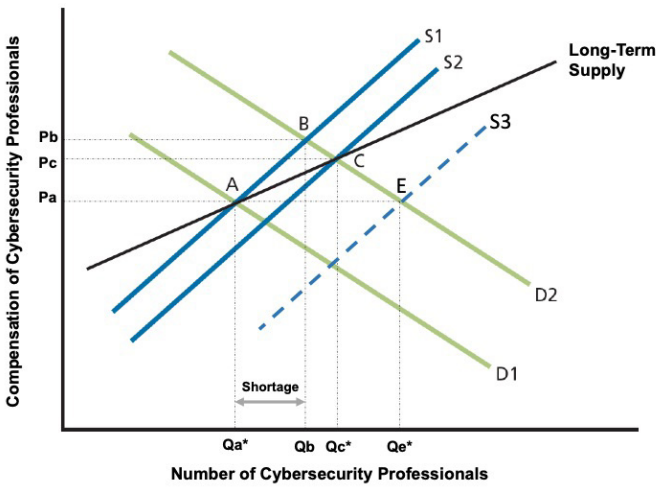
Analyzing the challenges facing the cybersecurity labor market helps countries prepare for conflict in cyberspace and helps organizations identify key gaps in the current workforce that can undermine business and industry objectives. Below we will analyze this labor market, provide a general and schematic characterization of cybersecurity labor supply and demand, describe the cybersecurity workforce, and identify a set of issues and challenges that should be addressed comprehensively by multiple stakeholders, especially in the Latin America and Caribbean region.

3.1. THE LABOR MARKET

From an economic perspective, the cybersecurity labor market follows the same principles as the free market, where the laws of supply and demand apply. The labor market is where supply and demand for jobs meet, where workers or the labor force provide the services demanded by employers.

The figure below presents a simplified view of the cybersecurity labor market. In the recent past, supply and demand met at point A (quantity of professionals Qa* with compensation of Pa). As shown, the demand for cybersecurity professionals has increased considerably. This increase may be due to multiple factors, including increased connectivity, increased digitalization, increased digital transformation, more economic activities in the digital environment, increased vulnerabilities, and others. These events pushed the demand curve to the right, from D1 to D2. The shift in the demand curve suggests that, as observed in the current market, many employers are willing to pay more (Pb) to hire the same quality and type of professional they were hiring before. The rise in demand has been further exacerbated in recent years due to the COVID-19 pandemic, and time is needed to develop more cybersecurity professionals in response to the increased demand.

Chart 7.
Cybersecurity labor market forces



Source: Adapted from RAND (RAND, 2014).

Training and education can take years to create a new equilibrium in the cybersecurity labor market. Even if individual workers in other occupations and in other sectors have the right set of skills to become cybersecurity professionals, they may not switch occupations or sectors immediately. Therefore, in the short run, the supply curve is quite inelastic; in other words, it is not very responsive to price. This situation also leads to shortages of professionals. For example, ISC2 estimates a shortage of between 515,000 and 701,000 professionals for the Latin America and Caribbean region (ISC2, 2021) (ISC2, 2022a). Point B can be seen as a short-term equilibrium and, in the long term, the market should reach a new equilibrium at point C (quantity of professionals Qc* with compensation of Pc).

As shown in the figure above, the long-run supply curve is likely to be more elastic (more price sensitive) than the short-run supply curves, because it is easier for people to move in and out of a profession in the longer term. For example, a new equilibrium could be found at point E (quantity Qe* with compensation of Pa) when the supply curve moves to the right from S2 to S3, there being more cybersecurity professionals in the market with lower compensation. However, shifts in the labor supply and demand curves along with the effects on gaps and prices depend on the actions taken by all the multiple stakeholders involved in the cybersecurity labor market.

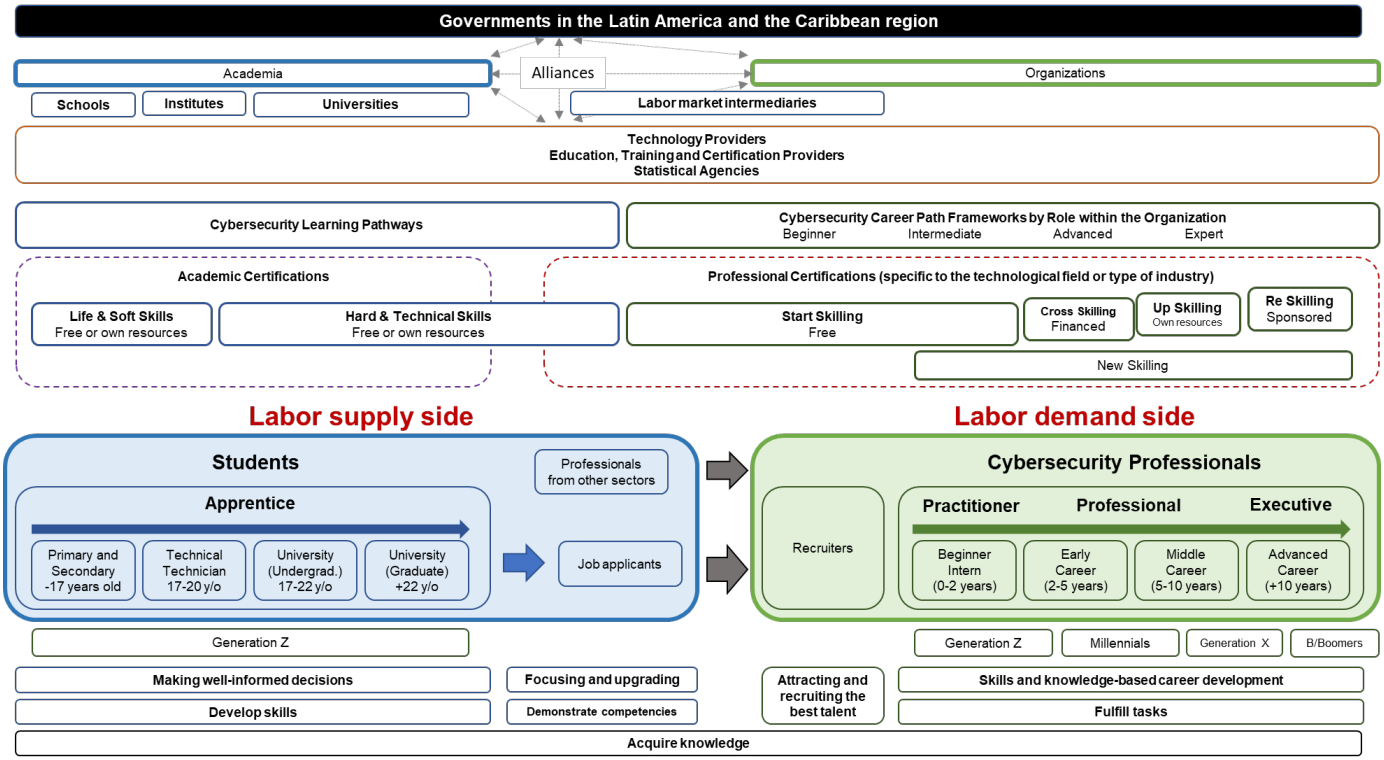
The figure below shows a general and schematic description of the supply and demand for cybersecurity labor in the region. First, the labor supply comprises: (i) recent graduates, (ii) professionals from other sectors or industries who may have technology expertise, and (iii) those who lack a technical background, but have other skills that can be applied in a cybersecurity-related job role.[28]

It is also important to consider current students who are at the primary, secondary, and tertiary levels of the region's educational systems, and even some at postgraduate levels. Generally, these students belong to Gen Z or "centennials,"[29] who have different characteristics from previous generations because they were born under new rules, guidelines, and concepts pertaining to the digital world.

These students should develop skills and make well-informed decisions, while job applicants should demonstrate competencies, be focused, and keep up to date.

28 On the labor supply side, there are at least six pathways to entry-level cybersecurity jobs: (i) apprenticeship route (high school with know-how), (ii) continuing education route (high school with certifications), (iii) first degree STEM route (undergraduate), (iv) first degree non-STEM route (undergraduate), (v) advanced degree route (graduate), and (vi) career switch route (CSES, 2018).
29 Persons born between 1997 and 2010.

Chart 8.
Schematic characterization of the cybersecurity labor supply and labor demand in the region



Source: Prepared by the authors.

The most representative stakeholder with an impact on the labor supply is academia, in particular schools, institutes, and universities. Given that students (future job applicants) are *sellers* in the cybersecurity labor market, whose value is determined by the skills they possess, academic institutions should provide them with the opportunity to develop a wide range of skills (life skills, soft skills, technical skills, and hard skills) to enter the cybersecurity field.

Moreover, labor demand is represented by organizations that need cybersecurity professionals, who can be classified as apprentices or trainees,[30] professionals, and executives, depending on how long they have been part of the workforce. This workforce includes people from several generations, for example, interns are generally Gen Z, professionals may consist of people from Gen Z, Gen Y, millennials,[31] or Gen X,[32] and finally, executives may be Gen X or baby boomers.[33]

Cybersecurity professionals in the workforce must accomplish tasks and develop a career based on skills and knowledge.

30 Around 1 in 3 cyber companies (27%) in the UK reported having offered apprenticeships or traineeships since the early 2020s (for a period of approximately 18 months) (DCMS & IPSOS, 2022).
31 People born between 1981 and 1996, called "digital natives," and the first generation that is truly global because they share the same values in all countries thanks to globalization and connection through the internet.
32 People born between 1965 and 1980, who have adapted very easily to the arrival of the internet in their lives and subsequent technological developments.
33 People born between 1946 and 1964, who have had to adapt to new technologies and are therefore considered "digital immigrants."

The most representative stakeholders with an impact on labor demand are public and private organizations in all economic sectors, which have human resources departments to identify, attract, and recruit talent. The labor market buyer represents the employer sector—whether public or private—and enters the labor market to purchase the services of a person who can perform the tasks demanded.

Finally, there are labor market intermediaries such as recruitment agencies and even professional network integration platforms. In addition, there are education, training, and certification providers and technology providers that offer tools, resources, and content to develop skills for both students and professionals, either through learning paths or through career pathways that provide academic[34] or professional[35] certifications, the latter being specific to the technological field or type of industry.[36] With support from these vendors, organizations can implement crosskilling, upskilling, reskilling, and new skilling plans, among others, to retain and maintain their cybersecurity workforce.

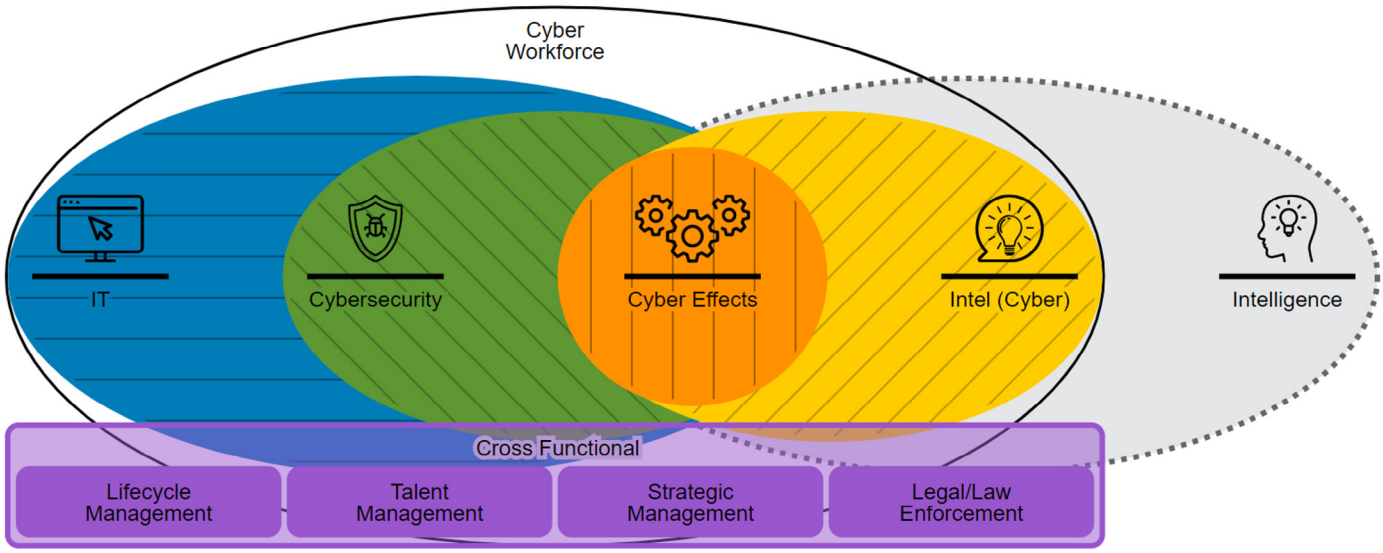
3.2. THE LABOR FORCE

According to the Cybersecurity Workforce Framework[37] of the National Initiative for Cybersecurity Education (NICE) of the National Institute of Standards and Technology (NIST), the cybersecurity workforce can be considered the pool of individuals possessing knowledge and skills to perform tasks required to achieve an organization's cybersecurity risk management objectives. These individuals may be internal or external to the organization.[38]

An example of workforce definition is shown in the "Cyber Career Pathways Tool"[39] based on the NICE Cybersecurity Workforce Framework and prepared by the National Initiative for Cybersecurity Careers and Studies (NICCS). The cybersecurity workforce is the set of professionals within an organization with the skills needed to: (i) build, secure, operate, defend, and protect technology, data, and resources, (ii) carry out related intelligence activities, (iii) enable future operations, and (iv) project power in or through cyberspace.

34 Academic certifications in cybersecurity are designed to provide students with in-depth training on some of the current issues in the field of cybersecurity. These courses are generally combined with other courses and certification programs to provide students with the skills and experience needed to get started in the growing cybersecurity industry.
35 Professional cybersecurity certifications are designed for individuals already working in the cybersecurity field (or closely related IT and networking fields) to receive training in some of the latest tools and software to detect, prevent, and combat cybersecurity issues. These certifications are used to demonstrate competence with specific technologies.
36 A roadmap of cybersecurity certifications can be found at: https://pauljerimy.com/security-certification-roadmap/
37 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1es.pdf
38 Around one-third of companies in the UK outsource some aspect of cybersecurity (DCMS & IPSOS, 2022)
39 https://niccs.cisa.gov/workforce-development/cyber-career-pathways-tool

Chart 9.
Schematic representation of an organization's workforce and its communities of professionals



Source: (NICCS, 2022).

According to the National Initiative for Cybersecurity Careers and Studies (NICCS, 2022), the workforce of an organization may be composed of the following communities of professionals with distinct but complementary skills:

A *Information Technology (IT):* professionals with the skills needed to design, build, configure, operate, and maintain IT, networks, and capabilities. This includes actions to prioritize portfolio investments; design, acquire, implement, evaluate, and dispose of IT, as well as the management of information resources; and the management, storage, transmission, and visualization of data and information.

B *Cybersecurity:* professionals with the skills needed to secure, defend, and preserve data, networks, net-centric capabilities, and other designated systems by ensuring that appropriate security controls and measures are in place and by taking internal defense measures. This includes access to system controls, monitoring, management, and integration of cybersecurity into all aspects of engineering and acquisition of cyber capabilities.

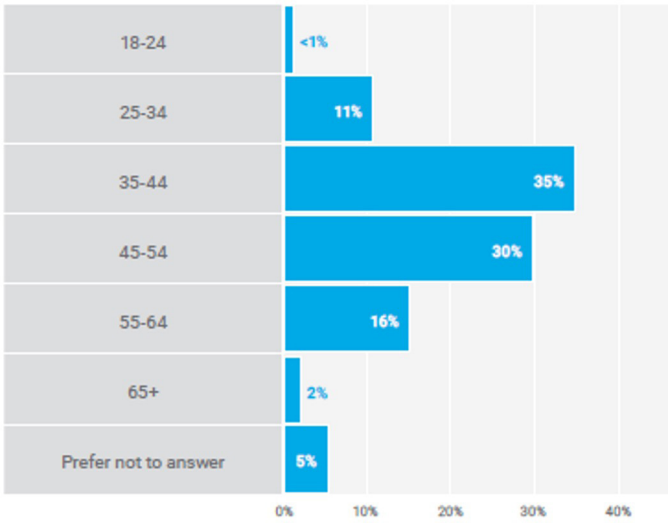
C *Cyber effects:* professionals with the skills needed to plan, support, and execute cyberspace capabilities where the primary purpose is to externally defend or conduct force projection in or through cyberspace.

D *Cyber intelligence:* professionals with the skills needed to collect, process, analyze, and disseminate information from all sources of intelligence on foreign actors' cyber programs, intentions, capabilities, research and development, and operational activities.

E *Cross-functional:* professionals with the skills needed to lead, acquire, and manage cyber initiatives; develop cyber workforce talent; and conduct cyber-related legal and law enforcement activities.

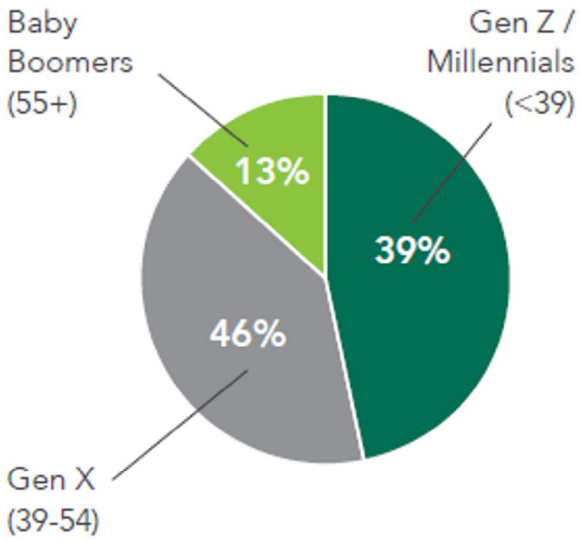
The workforce is currently made up of professionals between the ages of approximately 25 and 65.[40] This means that there is generational diversity, as they belong to the four demographic cohorts (Generations Z, Y, X, and baby boomers). These four generations of talent must not only coexist within organizations, but, with their own characteristics and differences, they must understand and complement each other.

Chart 10.
Labor force by age



Source: (ISACA, 2022).

Chart 11.
Representation by generation



Source: (ISACA, 2021).

The main sectors currently demanding cybersecurity professionals are the ICT sector, the financial and insurance sector, and the telecommunications sector. Public sector procurement also accounts for a larger share of the market in recent years.

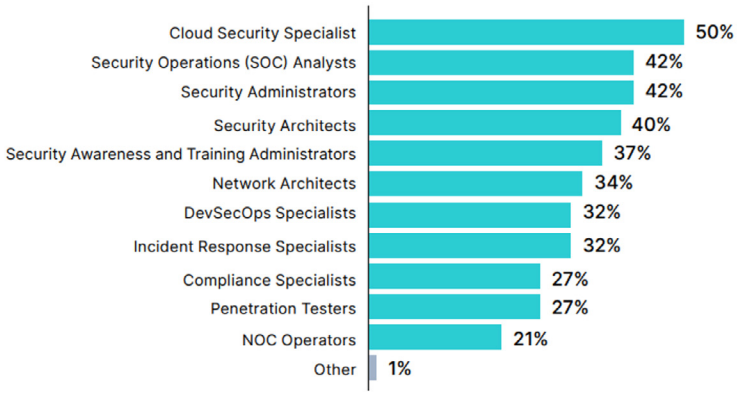
Chart 12.
Percentage of job advertisements for senior cyber roles from specific sectors in the UK

Note: From 8,426 cyber job postings between January and December 2021.
Source: (DCMS & IPSOS, 2022).

40 Notably, the majority (35%) are people between the ages of 35 and 44. It is emphasized that this situation may have an impact on the cybersecurity workforce as, according to (Cook, 2021), employees between the ages of 30 and 45 have driven the Great Resignation phenomenon, as they have seen the largest increase in resignation rates in the US, with an average increase of over 20% between 2020 and 2021.

A wide range of cybersecurity roles and specialties (specialists, analysts, and others) are in demand in the job market.[41] Some of the roles most in demand by employers in the US cybersecurity labor market include cybersecurity analyst, software developer, and cybersecurity consultant, among others.

Chart 13.
Top in-demand cybersecurity jobs



Source: (FORTINET, 2022).

Chart 14.
Top in-demand cybersecurity jobs in the US

Note: Data as of September 2022
Source: (CyberSeek, 2022).

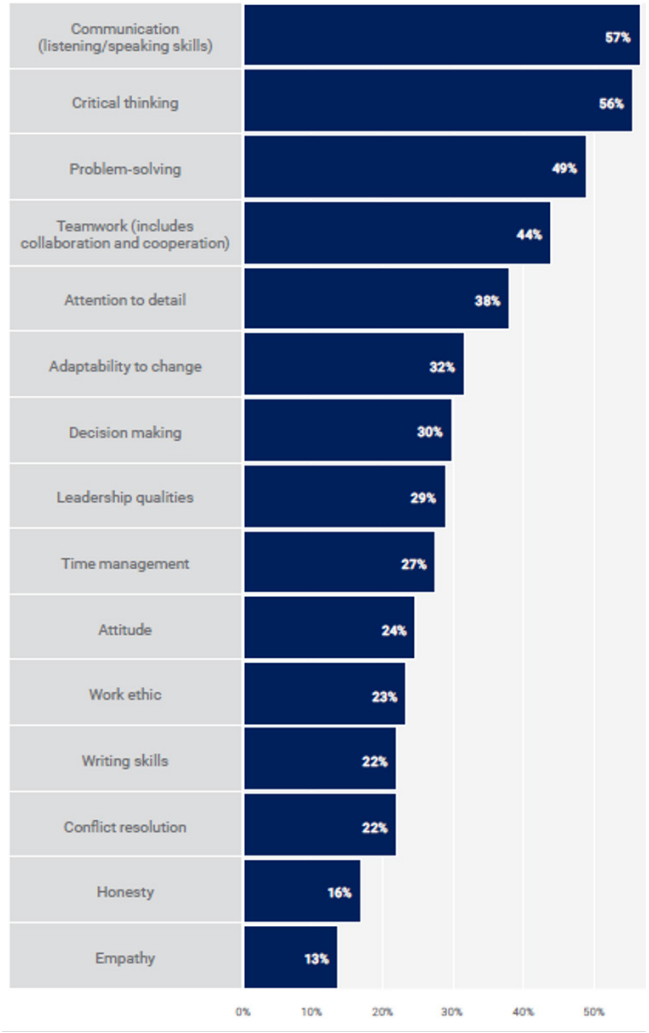
The main soft skills requirements in cybersecurity job descriptions in the UK are communication skills, creative thinking, problem solving, teamwork, and attention to detail. The top five soft skills most in demand in 2022 in Latin America and the Caribbean are adaptability, creative thinking, teamwork, emotional intelligence, and resilience (MichaelPage, 2022).

Chart 15.
Main attributes sought for cybersecurity personnel

Source: (ISC2, 2021)

41 According to CyberSeek, there were 714,548 online job postings in the United States for cybersecurity-related positions from May 2021 to April 2022 (CyberSeek, 2022); between January 2021 and December 2021 there were 153,192 job openings in cybersecurity in the UK (DCMS & IPSOS, 2022).

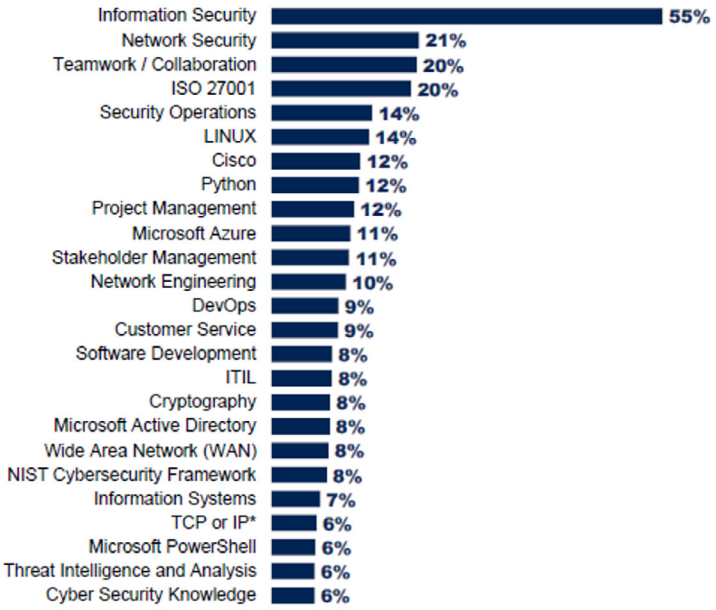
Chart 16.
Top soft skills for cyber roles in the cybersecurity industry



Source: (ISACA, 2022)

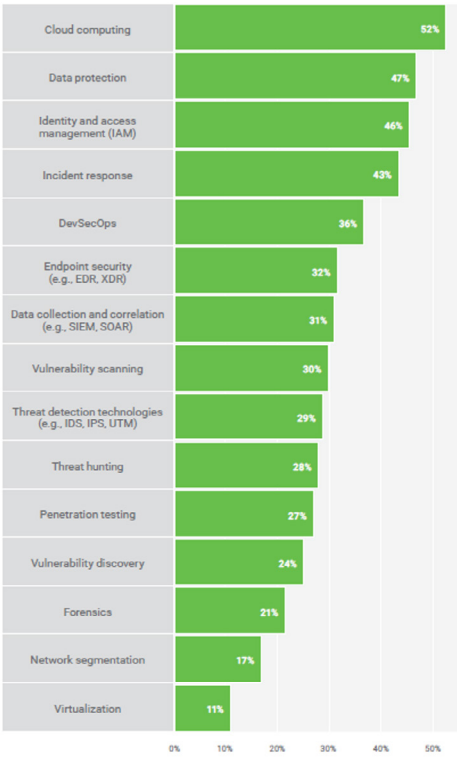
The main technical skills requirements in cybersecurity job descriptions in the UK are information security skills, network security skills, and skills related to standards, such as ISO 27001 (the international information security standard). Other technical skill areas required of cybersecurity professionals in the job market include cloud computing, development, security and operations (DevSecOps), risk management and technical controls, knowledge of operating systems and virtualization, cryptography, and programming.

Chart 17.
Top technical skills sought for senior cyber roles in the UK



From 35,103 cyber job postings between January and December 2021 requesting at least one specific skill.
Source: (DCMS & IPSOS, 2022).

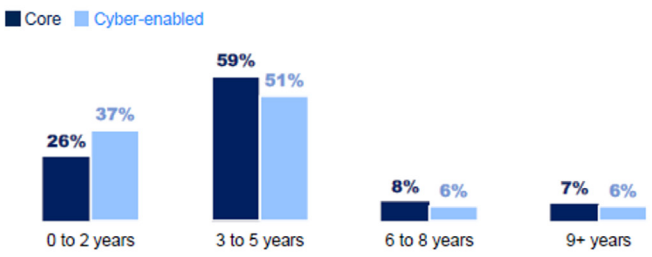
Chart 18.
Top technical skills for cyber roles in the cybersecurity industry



Source: (ISACA, 2022).

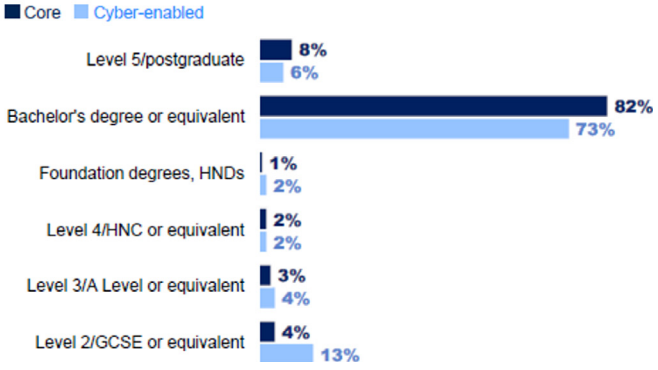
For the past several years, organizations have been seeking cybersecurity professionals with three to five years of experience, followed by entry-level applicants with a bachelor's degree or equivalent.

Chart 19.
Minimum experience levels required for cyber roles in the UK (senior and related roles)



Note: Based on 31,307 cyber job postings (main and related) between January and December 2021.
Source: (DCMS & IPSOS, 2022).

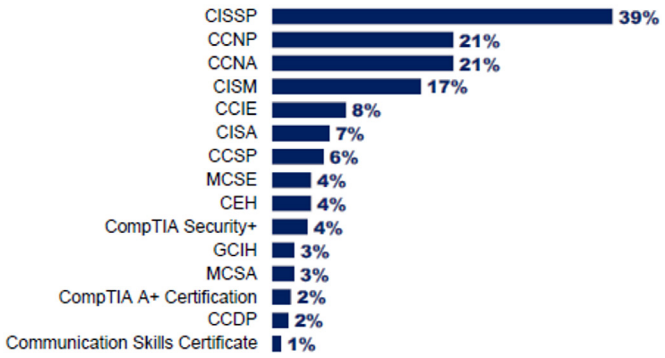
Chart 20.
Minimum education levels required for cyber roles in the UK (senior and related roles)



Note: From 30,472 cyber job postings (main and related) between January and December 2021.
Source: (DCMS & IPSOS, 2022).

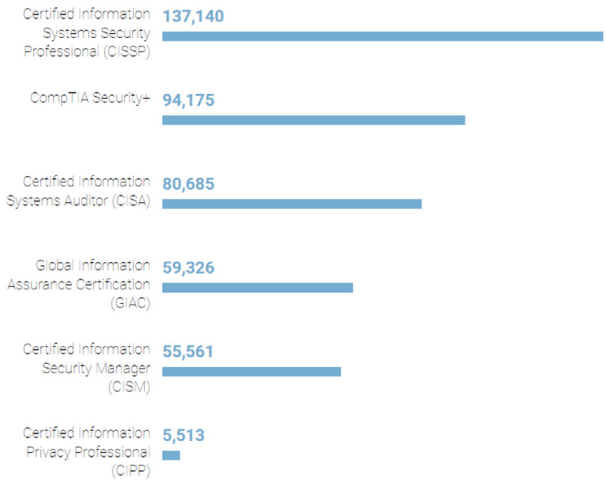
It is also important for available job candidates to be certified in information technology and information security. The *Certified Information Systems Security Professional (CISSP)* certification is the leading certification sought for key cyber roles globally. In the UK, Cisco Certified Network certifications like *Cisco Certified Network Professionals (CCNP)* and *Cisco Certified Network Associates (CCNA)* also continue to be in high demand. In the US job market, CompTIA Security+ and *Information Systems Audit and Control Association (ISACA)* certifications such as *Certified Information Systems Auditor (CISA)* and *Certified Information Security Manager (CISM)* are valued.

Chart 21.
Main certifications required for senior cyber roles in the UK



Note: From 11,086 cyber job postings between January and December 2021.
Source: (DCMS & IPSOS, 2022)

Chart 22.
Main certifications requested for senior cyber roles in the US



Note: Data as of September 2022.
Source: (CyberSeek, 2022)

Table 1.
Main Information Technology and Information Security Certifications

Provider		Certification	Cost
$(ISC)^2$	CISSP	Certified Information Systems Security Professional	US$ 749
ISACA	CISA	Certified Information Systems Auditor	US$ 575 ISACA members, US$ 760 nonmembers
ISACA	CISM	Certified Information Security Manager	US$ 575 ISACA members, US$ 760 nonmembers
CompTIA	Security+	CompTIA Security+	US$ 381
EC-Council	CEH	Certified Ethical Hacker	US$ 950 to US$ 1,199, depending on location
GIAC	GSEC	GIAC Security Essentials Certification	US$ 2,499
$(ISC)^2$	SSCP	Systems Security Certified Practitioner	US$ 249
CompTIA	CASP+	CompTIA Advanced Security Practitioner	US$ 480
GIAC	GCIH	GIAC Certified Incident Handler	US$ 2,499
Offensive Security	OSCP	Offensive Security Certified Professional	US$ 999 to US$ 5,499

Source: Coursera (2022) and ComputerScienceMS (2022)[43]

42 https://www.coursera.org/articles/popular-cybersecurity-certifications
43 https://computersciencems.com/resources/cyber-security/best-cybersecurity-certifications/

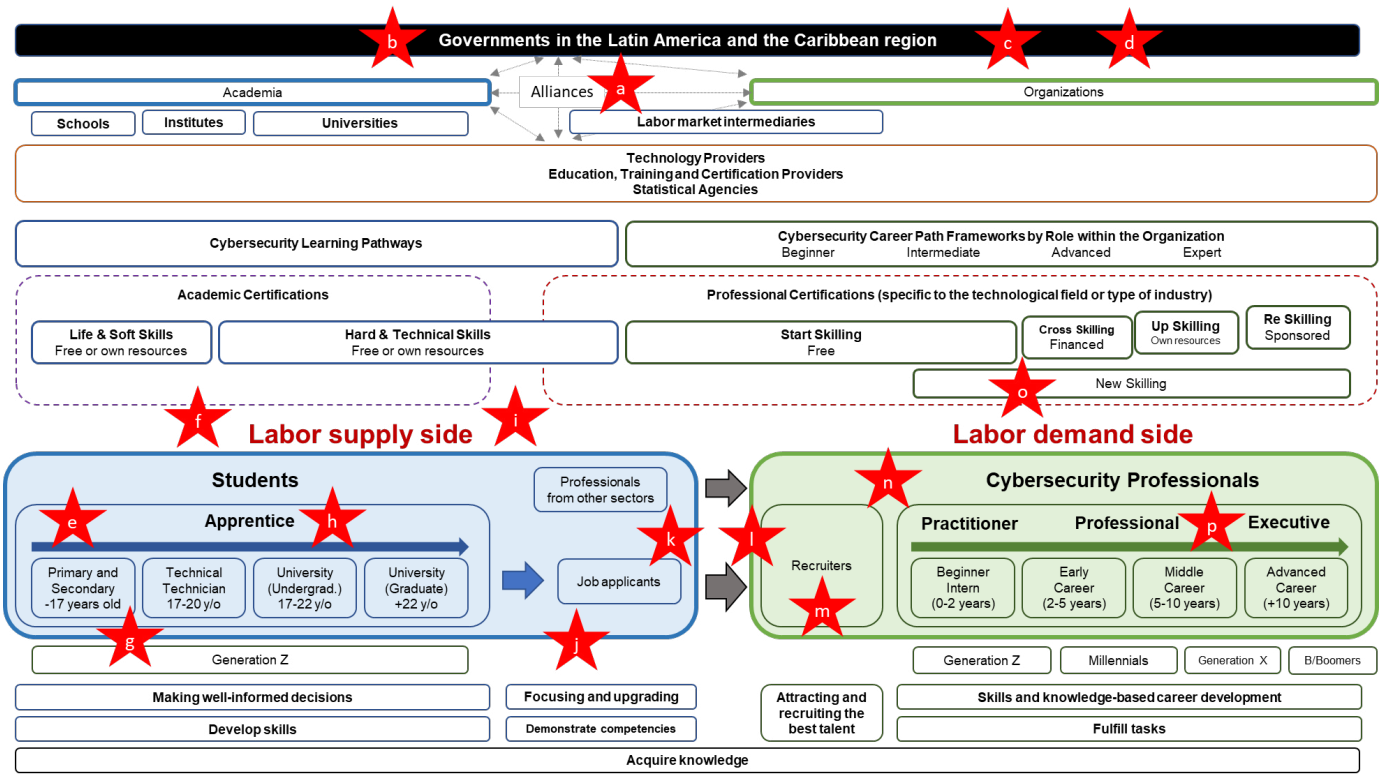
3.3. MAIN CHALLENGES

Strong cybersecurity skills and capabilities are a key driver of economic activity in the Latin America and Caribbean region and are fundamental to its future prosperity. The shortage of both cybersecurity professionals and cybersecurity skills may be caused by a unique combination of challenges for the region, where it is estimated that between 515,000 and 701,000 additional professionals may be needed for technical and nontechnical positions. As a result, the region is facing the following problem:

> ***Demand for cybersecurity professionals in Latin America and the Caribbean continues to outstrip supply, resulting in a growing gap (shortage) in the cybersecurity workforce.*** *These vacancies in public and private organizations can open the door to cyber threats, attacks, and incidents, with serious economic or social consequences, and can leave the countries of the region ill-prepared to face conflicts in cyberspace.*

The challenges in the cybersecurity labor market around this issue can be identified on both the labor supply side and the labor demand side. Some of the major challenges facing the countries of the region are outlined below.

Chart 23.
Schematic representation of the challenges in the region's cybersecurity labor market



Source: Prepared by the authors

The governments of the region face the following challenges:

- **A** Isolated efforts to develop the workforce and foster domestic and international partnerships
- **B** Weak regulatory framework and institutional coordination
- **C** Insufficient strategic information at the national level for decision-making
- **D** Insufficient awareness and outreach regarding resources, tools, and information for cybersecurity workforce development

On the cybersecurity labor supply side, the following challenges have been identified:

- **E** Insufficient development of STEM vocations and low digital skills among the region's children
- **F** Low/moderate English proficiency in the region
- **G** Lack of cybersecurity awareness and education at an early age
- **H** Lack of knowledge among students about educational opportunities
- **I** Disconnect between education, training, and industry
- **J** Lack of knowledge among job seekers about apprenticeship pathways
- **K** Poor understanding of the definition of the cybersecurity profession

On the cybersecurity labor demand side, the following challenges have been identified:

- **L** Lack of a common language between labor demand and labor supply
- **M** Organizations' preference for experience over qualifications
- **N** Gap in diversity, equity, and inclusion in the workforce
- **O** Difficulties in accessing career pathways
- **P** Inadequate retention programs in organizations

04

ANALYSIS FOR WORKFORCE DEVELOPMENT IN THE REGION

Despite the efforts of the countries in the Latin America and Caribbean region, many vacant cybersecurity positions remain unfilled because organizations cannot find the right talent. In response, education systems in the region have begun to mobilize, with a large number of educational institutions and entities creating and launching new cybersecurity degrees and courses. Similarly, *education, training* and *certification providers* and technology providers are strengthening their tools, resources, and content to develop the capabilities and skills of professionals in today's cybersecurity workforce.

However, the shortage of cybersecurity skills in the region is having an impact on the labor market and will continue to be serious in the medium term. To have strong cyber defenses, the region needs to build and develop a more diverse cybersecurity workforce with more and better technical and nontechnical skills. Improving gender balance will also help this workforce grow and mature. Strengthening the linkages between the skills offered by education systems and the needs of the labor market is a priority for closing human capital gaps in cybersecurity.

Accordingly, we present several considerations below from both the supply and demand sides of the labor market, with a view to fostering a cybersecurity ecosystem that will work comprehensively to develop the region's workforce. For each challenge identified, a three-part analysis is performed: a description of the importance of the issue addressed by the challenge, some support or evidence of the current situation at the global or regional level, and a description of good practices to address the challenge. Some considerations for the governments of Latin America and the Caribbean are also presented below.

4.1. THE LABOR SUPPLY SIDE

The new generation of students and professionals from other sectors need personal and professional skills to prepare them for current and future opportunities in the cybersecurity job market.

Based on the analysis of the challenges identified on the cybersecurity labor supply side, the considerations below are presented with a view to:

- Encouraging scientific vocations among children and young people in the region
- Strengthening English proficiency in the region
- Raising cybersecurity awareness and understanding at an early age
- Promoting access to educational opportunities
- Connecting education with training and industry
- Promoting access to learning pathways
- Clearly defining the cybersecurity profession

Encouraging scientific vocations among children and young people in the region

Relevance

Cybersecurity workforce development should start in primary and secondary schools. The more schools encourage students to consider a career in cybersecurity and the more they encourage early skills, the higher the quality of students in the tertiary education system will be. This means that schools should place greater emphasis on cybersecurity skills development in curricular and extracurricular programs as pathways to higher education. The skills learned in STEM education are the same skills required for a career in cybersecurity. Virtually all roles in the cybersecurity job market require STEM-related skills. As more workers with STEM-based skills enter the cybersecurity workforce, companies and other organizations are likely to see fewer successful cyberattacks and experience less economic harm from those attacks (WICKR, 2021).

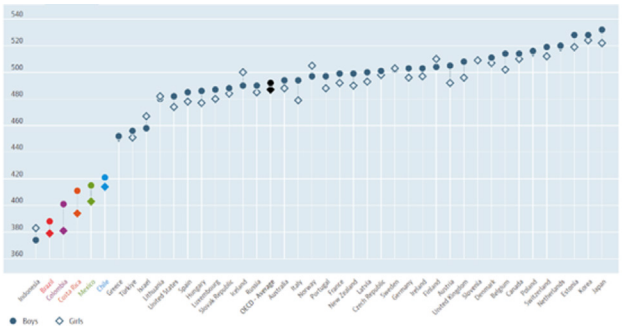
Challenges

In Latin America and the Caribbean, training in STEM knowledge areas is insufficient at the basic, middle, and secondary education levels. The results of the latest PISA measurement confirm that, on average, 15-year-old students in the region are three years behind in reading, mathematics, and science compared to a student in OECD countries. There is also a gender gap in the development of STEM skills (World Bank, 2019). Additionally, only 2.68% of those enrolled in higher education in the region are undertaking studies related to mathematics, science, and statistics. This is problematic when compared to the average for OECD countries, where enrollment in programs related to the same areas of knowledge reached 6.24% (DNP, 2022).

Some figures

Chart 24.

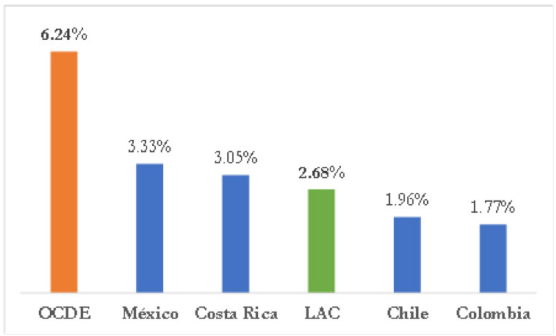
Mathematics performance differences (mean score) between boys and girls based on PISA 2018



Source: (OECD, 2022)

Chart 25.

Percentage of students enrolled in university programs in STEM fields



Source: (DNP, 2022)

Good practices

STEM education is a global effort to improve the scientific, technological, engineering, and mathematical skills of children and youth. Every country in the world has a different approach to implementing it. Some are integrating it into their educational policies; others are implementing it through external organizations. The *Estonian Education Strategy* (2021-2035)[44] emphasizes the STEM skills that create the most added value to enhance lifelong learning and retraining opportunities, including work-based learning. Singapore has introduced the *STEM Applied Learning Program (ALP)*[45] in its secondary schools in conjunction with STEM Inc., a unit of the Singapore Science Centre. Integrated STEAM education in South Korea is an approach for preparing a quality STEM workforce and literate citizens for a highly technological society by integrating science, technology, engineering, arts, and mathematics into education (Kang, 2019). At the regional level, the OAS offers the *Diploma in STEM-STEAM Education*[46] for teachers and education professionals to strengthen the design and implementation of STEM education practices, projects, and programs. Colombia has launched the 2022 *STEM Pathway Program*,[47] which aims to strengthen the capacities of 5,000 teachers and 100,000 elementary and middle school students in technology, science, engineering, and mathematics.

44 https://www.hm.ee/sites/default/files/haridusvaldkonna_arengukava_2035_kinnittaud_vv_eng.pdf
45 https://www.science.edu.sg/stem-inc/about-us/about-stem-inc
46 https://www.oas.org/en/scholarships/professionaldev/Courses_2022/Anuncio-PDSP-Educacion_STEM-STEAM.pdf
47 https://www.mineducacion.gov.co/portal/salaprensa/Noticias/410966:Gobierno-nacional-lanza-Ruta-Stem-2022-para-fortalecer-las-capacidades-de-docentes-y-estudiantes-del-pais-en-tecnologia-ciencia-ingenieria-y-matematicas

Strengthening English proficiency in the region

Relevance

English is the current default language in international business, diplomacy, entertainment, science, technology, and, in particular, cybersecurity. It is the most widely used language in the world by both native and non-native speakers. About 1.45 billion people (18.2% of the world's population) speak English, while approximately 548 million (6.9%) speak Spanish, and 258 million (3.2%) speak Portuguese (ETHNOLOGUE, 2022). English remains the most widely used language on the internet in 2022, representing 60.4% of all websites whose content language is known, while Spanish accounts for only 4.1% of websites (W3TECHS, 2022). In the world of computer programming and the software industry, English seems to be the lingua franca.[48] Most new codes are generally developed by English speakers. The most commonly used language in the leading academic and professional information technology and information security certifications is English.

Challenges

Central and South America have improved their English proficiency levels considerably over the last decade, but in 2022 it remains very low for Mexico and Haiti and low for Colombia, Ecuador, Panama, Venezuela, and Nicaragua (EF, 2022). The region also has the widest age-grade gap in the world. Young people's scores in the region have fallen significantly since 2020. School closures during the pandemic appear to be the most likely cause. Finally, in 2022, men's English proficiency has increased and women's has slightly decreased. Men have scored better than women in the region.

Some figures

Table 2.
Relevance of the English language globally

Spoken languages	WEB Sites by language *	Population by language **	Internet users by language ***
English	60.4%	18.2%	25.9%
Russian	5.4%	3.2%	2.5%
Spanish	4.1%	6.9%	7.9%
German	3.4%	1.7%	2.0%
French	3.1%	3.4%	3.3%
Japanese	2.8%	1.6%	2.6%
Chinese	1.8%	14.0%	19.4%
Other	19.0%	51.1%	36.4%
Total	**100.0%**	**100.0%**	**100.0%**

Source: Prepared by the authors based on * (W3TECHS, 2022), ** (ETHNOLOGUE, 2022), * (INTERNETWORLDSTATS, 2022)**

Chart 26.
Ranking of English proficiency in the region

Source: (EF, 2022)

Good practices

A bilingual person who speaks Spanish and English can understand one out of every three people connected to the internet (25.9% of internet users speak English and 7.9% speak Spanish). As a case of good practices, Argentina has implemented different initiatives and laws to improve language teaching in schools (National Education Law, Priority Learning Nuclei -NAP- and programs such as the Extended Day in Buenos Aires, etc.).[49] To achieve these objectives, a system for training language teachers in communicative methodologies has been developed. In Costa Rica, both the Bilingualism Guidelines[50] and the Educational Policy for the Promotion of Languages[51] highlight the importance of learning a second language as an indispensable tool for the training, performance, and personal and professional development of citizens, and propose to improve the teaching of English by introducing it at the preschool level.

48 https://preply.com/en/blog/b2b-english-for-software-engineers-developers-and-programmers/#:~:text=So%2C%20how%20important%20is%20English,will%20still%20be%20in%20English.
49 https://www.ambito.com/informacion-general/ranking/la-argentina-es-el-pais-mejor-dominio-del-ingles-america-latina-n5149683
50 Directive No. DM-0004-2-2019 and Administrative Order DVM-AC-004-2020 of the Ministry of Public Education of Costa Rica establishing provisions for the implementation of English language instruction at the preschool level.
51 http://cse.go.cr/sites/default/files/acuerdos/politica_educativa_para_la_promocion_de_idiomas.pdf

Raising cybersecurity awareness and understanding at an early age

Relevance

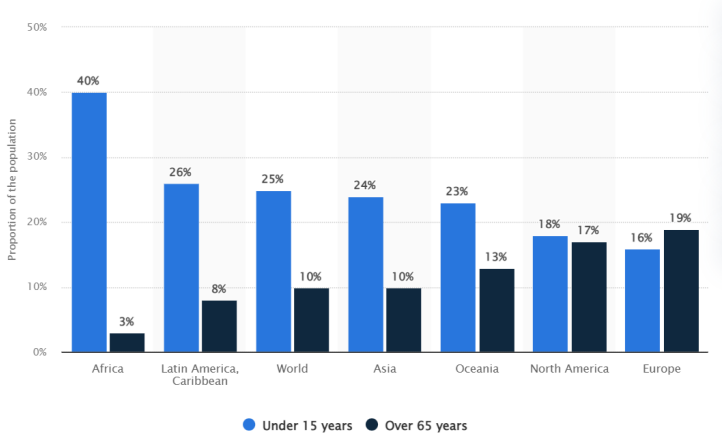
Twenty-four percent of the population of Latin America and the Caribbean is under the age of 15, compared to 18% in North America and 16% in Europe. Raising cybersecurity awareness and understanding at an early age is critical to workforce development in the region. Cyberattacks continue to target all types of organizations, including schools, as students and staff bring connected devices from home and share information across their networks. Raising awareness and teaching students at an early age about the risks they face online is important, but so is offering them the opportunity to learn about cybersecurity at a deeper level, enabling them to have lifelong cyber skills. It is imperative to close the growing gap in cybersecurity awareness and skills among young learners by ensuring that it becomes a critical subject area for education.

Challenges

Generally, in schools and other types of pre-college educational and vocational institutions, content related to cybersecurity risks is included as part of a technology subject area, such as computer science/IT/ICT/(digital) technology, or added to a variety of non-technology subjects. Early childhood education tends to be characterized by a lack of practical cybersecurity skills, the absence of a cybersecurity mindset, insufficient coverage in terms of a built-in skill-set oriented toward a cybersecurity-related career path, and a perceived general lack of interest and awareness among children in the development of cyber skills and cybersecurity as a potential career path (GFCE, 2022).

Some figures

Chart 27.
World population under 15 years of age and over 65 years of age
Source: STATISTA (2022)[52]



Good practices

Within international and multinational contexts, a broad range of cybersecurity educational content is available in pre-university settings through programs, guidelines, and initiatives. One notable example, the *Child Online Protection (COP)*[53] program of the International Telecommunication Union (ITU) is aimed at children, parents and educators, industry and policy makers. The content provided by the European Union Agency for Cybersecurity (ENISA) also focuses in part on raising awareness and understanding of cybersecurity.[54] The European Cybersecurity Organization (ECSO) is developing the *Youth4Cyber*[55] initiative, which aims to educate and raise awareness of cybersecurity among young people (ages 6 to 26). Also noteworthy is the content of the Global Forum on Cyber Expertise (GFCE),[56] where best practices are shared and initiatives are developed to improve cyber capacity. At the national level, the *SG Cyber Youth* program in Singapore led by the Cyber Security Agency of Singapore (CSA) to guide children and youth (especially those in secondary schools) toward a career in cybersecurity, with the support of academia, the community, and industry, is of particular note. Also, the US Cybersecurity Education and Training Assistance Program (CETAP)[57] supports cybersecurity education in K-12 classrooms through cybersecurity curriculum development and instructor training.[58]

52 https://www.statista.com/statistics/265759/world-population-by-age-and-region/#:~:text=Globally%2C%20about%2026%20percent%20of%20the%20world%20is,19%20percent%20being%20over%2065%20years%20of%20age.
53 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP/COP.aspx and https://www.itu-cop-guidelines.com/
54 https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide/at_download/fullReport
55 https://www.ecs-org.eu/initiatives/youth4cyber
56 https://thegfce.org/working-groups/working-group-d/
57 https://niccs.cisa.gov/education-training/cybersecurity-teachers
58 K–12 ("k through twelve") is the designation used in some educational systems for primary and secondary schooling.

Promoting access to educational opportunities

Relevance

Higher education offers a broad range of content, courses, modules, and opportunities to explore cybersecurity at both the undergraduate and graduate levels. Universities and institutes of higher education are rapidly expanding their offerings of cybersecurity programs by awarding specific degrees or specializations or master's degrees in IT, ICT, and information security. As the demand for cybersecurity professionals has grown in recent years, higher education has also responded by providing: (i) dedicated cybersecurity courses, (ii) general computer science courses with one or more modules in cybersecurity, and (iii) nontechnical courses with modules in cybersecurity. Multidisciplinary courses are also becoming increasingly common.

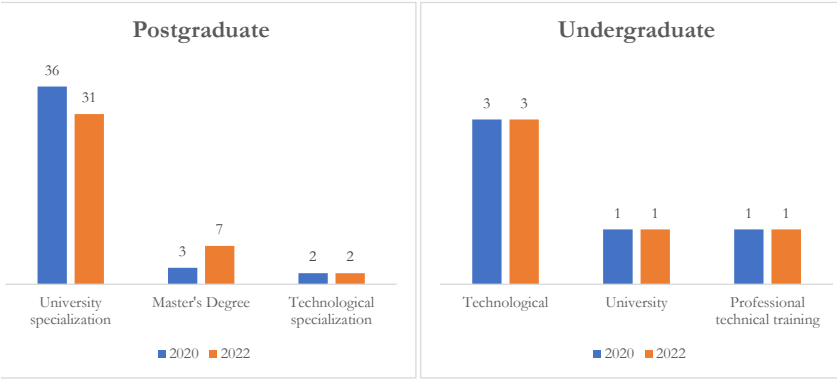
Challenges

Although isolated efforts are underway in several countries,[59] there is not enough education in the region to generate adequate cybersecurity skills and capabilities.[60] Demand for cybersecurity education from postsecondary students is not increasing fast enough. In addition, the demand for cybersecurity skills in industry sectors makes it difficult for academia to attract academics, researchers, and professors with knowledge, practical experience, research backgrounds, and academic aspirations. There are also difficulties in attracting and retaining qualified cybersecurity faculty, largely because such high-quality professionals command above-average salaries. Tertiary education providers should ensure that cybersecurity is considered a desirable study option in order to attract the best and most motivated students.

Some figures

Chart 28.
Changes in the number of higher education programs related to cybersecurity and information security in Colombia

Source: Data from 2020 (DNP, 2020) and Data from 2022[61] (MINEDUCACION, 2022)



Good practices

In the promotion of educational offerings, regional initiatives for the development of cybersecurity skills such as ENISA's CYBERHEAD stand out.[62] It has become the largest validated database of higher education in cybersecurity (123 programs in 25 countries), and the main point of reference for all citizens in the region seeking to improve their cybersecurity knowledge and skills. In the United Kingdom, the National Cyber Security Centre (NCSC) has certified several bachelor's and master's level degrees under the certificate degree program. It has also supported the development of Academic Centers of Excellence in Cybersecurity Research (ACE-CSR) and Academic Centers of Excellence in Cybersecurity Education (ACE-CSE). Singapore has several programs aimed at young people, especially the *SG Cyber Youth*[63] program that provides them with guidance to get started in cybersecurity, with the support of academia, the community, and industry. One key initiative is the *Youth Cyber Exploration Programme,*[64] which introduces high school students to the basics of cybersecurity and cultivates their interest in a career in cybersecurity. The *Cybersecurity Career Mentoring Programme (CCMP)* also provides career guidance and support from mentors in the industry. Other initiatives in Singapore include the *Student Volunteer & Recognition Programme (SVRP)* and the *Cybersecurity Learning Journeys.* There is also the *SG Cyber Olympians* program, which prepares students through cyber warfare training sessions, more in-depth training, and international competitions.

59 For example, the 2022 Course Directory of the Cyber-Security Hub of the city of Córdoba in Argentina (https://corlab.cordoba.gob.ar/wp-content/uploads/2022/09/oferta-educativa-ciberseguridad-cordoba.pdf)
60 For example, according to Colombia's National Department of Planning (DNP), *"it is clear that few educational programs related to digital security are offered at the undergraduate academic level"* in Colombia (DNP, 2020).
61 A number of master's degree programs are currently offered in Colombia, including master's degrees in information management and security; digital security; information security; computer and communications security; cybersecurity and computer forensics; and cybersecurity and cyber defense.
62 https://www.enisa.europa.eu/topics/cybersecurity-education/cyberhead#/
63 https://www.cyberyouth.sg/
64 https://www.csa.gov.sg/ycep

Connecting education with training and industry

Relevance

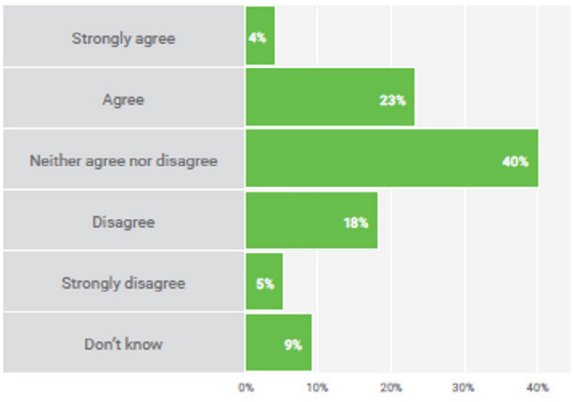
The development of higher and continuing education curricula and programs is crucial for mitigating the labor shortage and cybersecurity skills gap. They encourage students to pursue cybersecurity topics, enhance the operational capabilities of potential entrants into the workforce, and promote and foster relationships between academia and industry, as well as align cybersecurity training with real industry needs. Curricula should be multidisciplinary, as students and professionals need to understand a variety of cybersecurity knowledge areas, ranging from more technical topics to social and legal aspects. In addition, plans and programs should prioritize practical training over theory-based training.

Challenges

The countries of the region have no specific frameworks for defining standardized curricula that are widely agreed upon and aligned with industry. There is no evidence of partnerships between industry and academia to generate national curricular guidelines for undergraduate or graduate programs related to cybersecurity or information security. A set of core subject areas with their associated cybersecurity practices in which all students are expected to be proficient by the end of secondary and tertiary education needs to emerge periodically from such partnerships. This situation can have an impact on students' entry into the workforce.

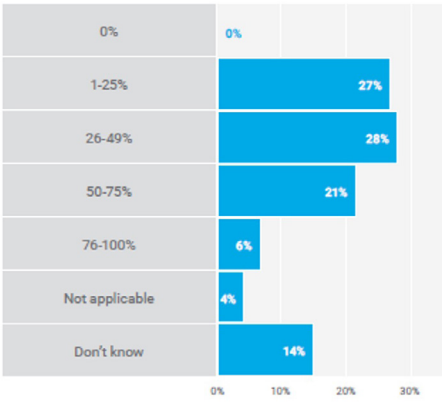
Some figures

Chart 29.
Are recent college graduates in cybersecurity well prepared for cybersecurity challenges in your organization?



Source: (ISACA, 2022)

Chart 30.
% of cybersecurity applicants who are well qualified for the position for which they are applying



Source: (ISACA, 2022)

Good practices

Some initiatives are underway to help create specific frameworks or a standardized set of guidelines for countries to follow for pre-university and university education. As for pre-university education, the *Informatics for All*[65] initiative and its *"Informatics Reference Framework for School"*[66] launched in 2022 is a good example of how different stakeholders in various countries can work together to produce more standardized and widely adopted curricula and guidelines. For university education, the United States has seen several public-private collaboration efforts, most notably the Joint Task Force (JTF) on Cybersecurity Education, which has been working since 2015 to develop a curriculum guide that aligns undergraduate cybersecurity academic programs with industry needs. Special mention should also be made of the *Cyber2yr2020*[67] project, which focuses on curriculum guidelines for cybersecurity programs, including career-oriented associate degree programs that should align with the NIST National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.

65 https://www.informaticsforall.org/
66 https://www.informaticsforall.org/wp-content/uploads/2022/03/Informatics-Reference-Framework-for-School-release-February-2022.pdf
67 http://ccecc.acm.org/files/publications/Cyber2yr2020.pdf

Promoting access to learning pathways

Relevance

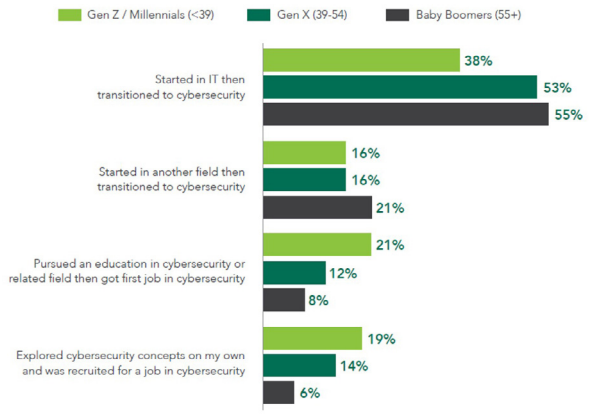
Having a solid base of knowledge and skills is imperative in the cybersecurity job market. This includes soft skills, such as verbal and written communication, and technical skills validated through academic or professional certifications. Students and professionals from other sectors who will become job seekers can develop these skills and competencies through learning pathways specifically focused on entry-level or trainee levels within organizations. Both *education, training,* and *certification providers* and technology providers are key players in bridging the gap between demand and supply in cybersecurity skills. These tracks, consisting of hands-on courses that teach business and technology skills, allow people to demonstrate their skills to prospective employers. Academic certificate programs in cybersecurity are emphasized for students who have already earned a degree in a related field and are looking to change careers, or for students who want to explore what it would be like to prepare for a career in cybersecurity before committing to a longer-term course of study.

Challenges

Starting and advancing a career in cybersecurity is not as straightforward as other more traditional professions. It is important to generate more interest in the countries of the region among students and job seekers so they can enter the learning pathways at their own pace. Stakeholders may be unable to encourage more students to pursue academic paths more readily associated with a job in cybersecurity. Another problem is that the skills required are changing at a faster pace than usual within advanced technology fields, due to the changes introduced by new digital technology and the rapid digitalization of society.

Some figures

Chart 31.
Pathways to careers in cybersecurity



Source: (ISC2, 2021)

Chart 32.
Cybersecurity team composition by experience level by organization size

Source: (ISC2, 2022b)

Good practices

The labor market has key players that promote learning pathways from the labor supply side. *Education, training,* and *certification providers* and technology providers offer content at all levels of complexity to develop capabilities and skills. The Massive Open Online Course (MOOC)[68] market offers many learning opportunities for students and professionals. Examples of such platforms include Coursera (https://www.coursera.org/), LinkedIn Learning (https://www.lynda.com/), edX (http://www.edx.org/), PluralSight (https://www.pluralsight.com/), Cybrary (https://www.cybrary.it/), Udacity (https://www.udacity.com/), Udemy (https://www.udemy.com/), MiriadaX (https://miriadax.net/) and Cyberwiser (https://www.cyberwiser.eu/). Also of note are platforms offered by technology providers to initiate learning pathways, such as the *Cisco Networking Academy,* which has developed *Skills for All,*[69] a free, mobile platform that delivers self-paced learning experiences to drive an inclusive future for all, including the *Cybersecurity Learning Pathway.*[70]

68 The term MOOC is an acronym for *Massive Open Online Courses*, i.e., it refers to open online courses, both free and paid, that are accessible to a massive number of learners.
69 https://skillsforall.com/
70 Being aligned with the new *Certiport Information Technology (IT) Specialist in Cybersecurity* certification, trainees can perform roles such as cybersecurity technician, junior cybersecurity analyst, and help desk support. Graduates can also take advantage of CISCO's *Talent Bridge* program and use the job search engine that includes opportunities at more than 725 employer partners in 70 countries.

Clearly defining the cybersecurity profession

Relevance

The role of cybersecurity professionals is constantly evolving and, therefore, the cybersecurity profession is difficult to define. The taxonomy around cybersecurity can also be confusing, and the routes to and through cybersecurity careers can be difficult to navigate. It is important for countries to address this issue to ensure that there is a structured and sustainable cybersecurity profession. The technical language and acronyms that are often used can make this challenge especially steep for those students or job applicants who are new or unfamiliar with cybersecurity. The current professional landscape is also complex for existing professional organizations and *education, training,* and *certification providers*, which are often unable to articulate the equivalence of their offerings absent a common technical framework. Cybersecurity is increasingly recognized as a highly interdisciplinary topic, encompassing knowledge areas such as risk management and governance, cyber laws and regulations, human factors, protection of privacy and online rights, and adversarial behaviors (GFCE, 2022).

Challenges

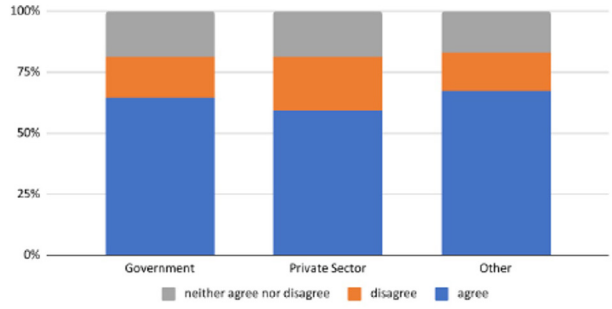
In the region, *computer security* and *information security* are terms that are still confused with the term *cybersecurity*. This also creates confusion among students and job applicants regarding the scope of work and the skills they must possess to meet requirements or profiles when seeking employment. More than half of the stakeholders surveyed in a global study on the development of cybersecurity as a profession mentioned that the definition of the profession is unclear (GFCE, 2022). This response was virtually the same across all stakeholder groups and was slightly higher among respondents from developed countries.

Some figures

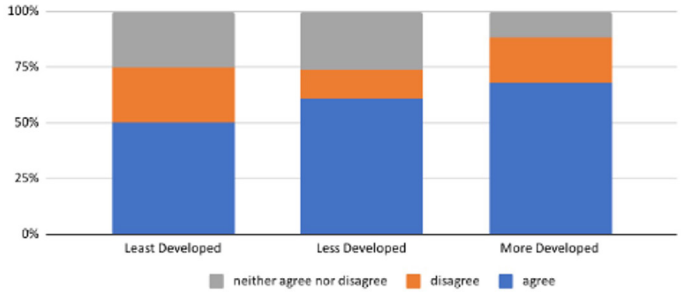
Chart 33.

Perceptions regarding the definition of the cybersecurity profession

(To what extent do you agree that the definition of cybersecurity professional is unclear?)



Source: (GFCE, 2022)



Source: (GFCE, 2022)

Good practices

In the United Kingdom, the *UK Cyber Security Council* and the *Cyber Security Body Of Knowledge (CyBOK)*[71] have established a system to categorize[72] of cybersecurity roles. The CyBOK is a unique resource, providing a core body of knowledge that spans the breadth and depth of cybersecurity across a wide range of disciplines. For example, according to (DCMS & IPSOS, 2022), the most in-demand cybersecurity roles in the UK are security engineers (35%), security analysts (18%), security managers (14%), security architects (11%), and security consultants (9%). There are initiatives for specific topics; for example, Singapore has issued an *Operational Technology Cybersecurity Competency Framework* (CSA, 2021) which lays the foundation for attracting and developing talent for the emerging OT cybersecurity sector in Singapore and provides guidance on competencies to equip professionals to perform their jobs in the OT industry sectors. Other initiatives include the (ISC)[2] CBK[73] (Body of Knowledge), which is a peer-developed compendium of what a competent cybersecurity professional should know, including the skills, techniques, and practices routinely employed. It establishes a common framework of information security terms and principles that enables cybersecurity and IT/ICT professionals around the world to discuss, debate, and resolve issues related to the profession with a common understanding, taxonomy, and lexicon.

71 https://www.cybok.org/

72 For example, the cyber workforce in the UK works in particular roles or specialties: cybersecurity generalist roles (26%); security governance, risk, compliance and legal (14%); network security (networks and firewalls) (11%); security architecture (11%); incident management, response, and recovery (10%); security operations (e.g., intrusion detection) (9%); system security (operating systems and patching) (9%); and penetration testing (8%) (DCMS & IPSOS, 2022).

73 https://www.isc2.org/Certifications/CBK

4.2. THE LABOR DEMAND SIDE

Organizations have become increasingly reliant on technology and protecting systems, networks, and data against cyberattacks is more challenging than ever, with even more security technologies and processes that must work together. Therefore, organizations need their cybersecurity workforce to be larger and have a wider range of skills than ever before.

Based on the analysis of the challenges identified on the labor demand side of cybersecurity, the following considerations are presented with the aim of:

- Ensuring that demand and supply speak a common language
- Adjusting hiring requirements to attract top talent
- Promoting diversity, equity, and inclusion in the workforce
- Promoting career pathways
- Retaining the workforce

Ensuring that demand and supply speak a common language

Relevance

As the cybersecurity labor market has matured, a local and regional need has arisen for a common lexicon to describe and organize the cybersecurity workforce. It is important for countries to have frameworks in place that will create a common understanding of the roles, competencies, skills, and knowledge used by and for individuals, employers, and *education, training,* and *certification providers* to address the cybersecurity skills shortage. It also helps to further facilitate the recognition of cybersecurity-related skills, boosting employment and employability in cybersecurity-related positions. These frameworks, which in several countries have become standards, provide guidance on what roles to implement in an organization to accomplish necessary cybersecurity tasks and on how to identify the right talent by formulating appropriate job descriptions that correctly identify the right qualifications and duties that can be assigned to each role.

Challenges

There have been no clear efforts at standardization in the region in terms of how cybersecurity roles and associated skills are defined and described, and how the workforce is trained. The lack of unified standards for the knowledge, competence, and skills that students must develop to meet the needs and that organizations must consider when creating their talent search profiles can create inefficiencies in the cybersecurity labor market, affecting seller-consumer transactions in this market.

Some figures

Chart 34.
Benefits of the European Cybersecurity Skills Framework

Source: (ENISA, 2022)

Good practices

A good practice in the Americas is NIST's National Initiative for Cybersecurity Education (NICE) cybersecurity workforce framework that provides employers, employees, educators, students, and training providers in the United States with a common language for defining cybersecurity work. By defining the cybersecurity workforce and using standard terminology, academia and employers can synchronize education, recruitment, and development to establish a strong talent pipeline and maintain a highly skilled workforce. For example, the *National Initiative for Cybersecurity Careers and Studies* has developed *Cyber Career Pathways Tool,*[74] based on the NICE framework, which describes the workforce by detailing the key attributes among each of 52 defined cybersecurity job roles.[75] Another good practice is the development of a *European Cybersecurity Skills Framework*[76] by ENISA. Australia has devised a *Cyber Skills Framework*[77] that enables targeted recruitment of cyber specialists, provides a development pathway for current and future cyber personnel, and aligns skills, knowledge, and attributes with national and international industry standards.

74 NIST has also issued documentation (Draft NISTIR 8193) on capability indicators intended to help organizations determine whether a cybersecurity worker can perform a cybersecurity job role. Capability indicators are recommended education, certification, training, experiential learning, and continuous learning that could signal an increased ability to perform a given work role.
75 https://niccs.cisa.gov/about-niccs/workforce-framework-cybersecurity-nice-framework-work-roles
76 https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework
77 https://www.cyber.gov.au/acsc/view-all-content/publications/asd-cyber-skills-framework

Adjusting hiring requirements to attract top talent

Relevance

Hiring processes are step-by-step methods for finding, recruiting, and hiring new employees. A good hiring process helps attract and retain high quality employees in the cybersecurity workforce. The specific elements of a hiring process are unique to each organization. Hiring managers rely on a wide range of tactics and resources to recruit all entry-level and junior-level personnel. While recruitment firms and certifying bodies rank high across all countries, apprenticeships and internships are more popular in the UK and India (ISC2, 2022b).

Challenges

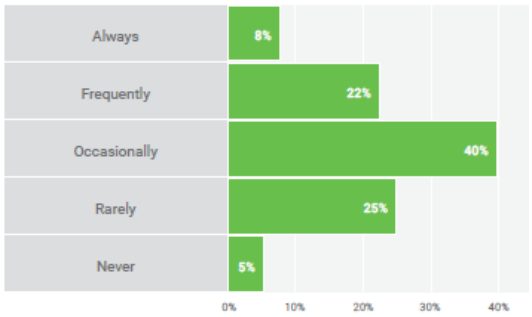
Hiring talent for cybersecurity roles continues to be a challenge for many organizations. Communication problems persist between organization managers and their human resources departments (ISACA, 2022). In addition, job specifications are different if the organizations operate outside the cybersecurity industry. Employers also have high expectations about the skill level of candidates. In many instances, organizations are looking for cybersecurity professionals for entry-level jobs, yet they are unwittingly asking for several years of experience. Assumptions by some employers that candidates must have a certain academic degree or certification to qualify for a cybersecurity job or role, or that promotions should be based on time in service rather than competencies, are barriers to attracting top talent. Other problems are that employers sometimes ask for talent that is not needed, and they often dismiss people who lack formal credentials despite evidence of their having acquired cybersecurity skills and knowledge. Recruiting agents in the UK say they commonly saw poorly written job specifications that attempted to recruit multiple roles into one, did not reflect the actual requirements for the role being offered, or minimized important benefits such as training (DCMS & IPSOS, 2022).

Some figures

Chart 35.

Understanding of human resources hiring needs

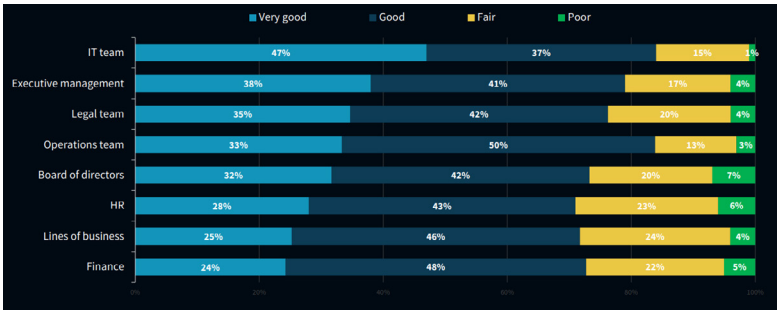
How often do you feel your HR department fully understands your cybersecurity hiring needs to properly shortlist candidates?



Source: (ISACA, 2022)

Chart 36.

Estado de la relación entre la ciberseguridad y otras organizaciones funcionales



Source: (ESG, 2021)

Good practices

Job descriptions should be a shared responsibility. It is important to continually improve the relationship between cybersecurity and human resources to create realistic job descriptions for entry-level and junior roles that set clear expectations for new employees and employers (ISC2, 2022b). It is important to create job postings that will appeal to those who are coming out of cybersecurity training and education programs or who have self-developed. Organizations need to redefine the minimum requirements for obtaining an entry-level cybersecurity job and embrace nontraditional training channels. CISCO has developed a matching engine called *Talent Bridge*[79] that automates the connection between the students from the *Cisco Networking Academy* and a network of partners around the world, at no cost to employers or students. The engine matches students' qualifications with employers' needs, making it easier for hiring managers to quickly identify top candidates.

78 For example, one of the most sought-after certifications is the CISSP, which requires candidates to pass the exam and have at least five years of cumulative paid work experience in two or more of the eight ISC2 domains. When they ask for this certification, employers are actually requiring five years of experience for an entry-level position.
79 https://www.netacad.com/es/careers/matching-engine

Promoting diversity, equity, and inclusion in the workforce

Relevance

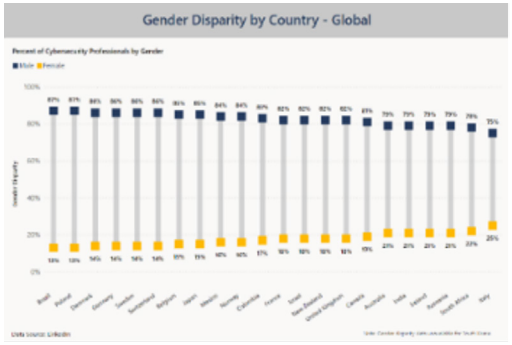
The current challenge in the labor market is not only to hire more people, but also to build more capable and diverse teams (FORTINET, 2022). While businesses need qualified talent for a variety of roles, 89% of global companies also have explicit diversity goals as part of their hiring plan. A more diverse cybersecurity team is a better cybersecurity team, as in this multidisciplinary field different perspectives are critical. When threats change every day, the diverse views of the workforce help to counteract them by bringing new ideas to situations. In some places, like the UK, the cyber workforce has become more diverse over the last three years in terms of the number of women and ethnic minorities working in cyber roles.[80]

Challenges

According to the latest report from ASPEN's digital technology policy center, underrepresented groups such as African-American (9%), Hispanic (4%), and Asian (8%) professionals make up a shrinking percentage of the industry. Similarly, women make up 51% of the population, but account for only 24% of the cybersecurity workforce (ASPENDIGITAL, 2021). Globally, 70% of IT managers see the hiring of women and new graduates as one of their top three challenges. Although organizations in Latin America (93%) and North America (90%) have established diversity objectives, probably because of greater difficulties in recruiting from these populations, the diversity targets are not always met (FORTINET, 2022).

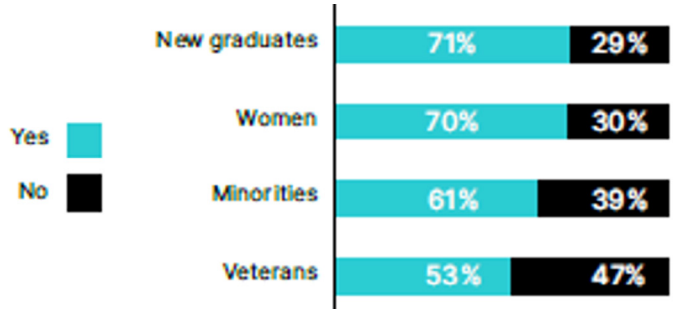
Algunas cifras

Chart 37.
Gender disparity in cybersecurity



Source: (MICROSOFT, 2022)

Chart 38.
Is hiring from these populations one of your organization's top three challenges?



Source: (FORTINET, 2022)

Good practices

The UK highlights the importance of having champions for diverse cyber recruitment, within organizations and across the industry, to help change the culture among employers and raise awareness of the needs of diverse candidates (DCMS & IPSOS, 2022). Another good practice in organizations is to add inclusive language in job descriptions that explicitly indicates interest in minority groups such as people of color and members of the LGBTQIA+ community.[81] These practices foster welcoming environments for the workforce and the personal and professional development of cybersecurity talent. Singapore has initiatives such as SG Cyber Women,[82] aimed at leveraging the underrepresented talent pool, from as early as tertiary education, to join the cybersecurity profession. At the regional level, CISCO is currently offering free training in three phases to the entire community of Chilean women under the *Connected and Safe Chilean Women's Cybersecurity Educational Program*[83] seeking to accelerate digital transformation and gender inclusion in Chile. Finally, WOMCY[84] is an initiative that seeks to increase diversity in cybersecurity in the Latin America and Caribbean region by minimizing the knowledge gap and increasing opportunities for women in the cybersecurity industry.

80 There is evidence that the cyber workforce in the UK has become more diverse in the last three years, both in terms of gender (22% are women, up from 15% in 2020) and ethnicity (25% are from ethnic minorities, up from 16% in 2020). The senior workforce (typically those with six or more years of experience) tends to be somewhat less diverse than those in younger roles, in terms of gender, ethnicity, and disability status. For example, only 13 percent of senior-level positions are held by women. There has been an increase in efforts to recruit people with neurodiverse conditions (23% of cyber employers have made changes for this group versus 15% in 2021) However, organizations that make accommodations to encourage any of these diverse groups to apply are still in the minority (DCMS & IPSOS, 2022)
81 LGBTQIA+ is the acronym for Lesbian, Gay, Bisexual, Transgender, Intersex, Queer/Questioning, Asexual.
82 https://www.csa.gov.sg/programmes/sgcybertalent/sgcyberwomen
83 https://www.cisco.com/c/m/es_cl/cda/chilenas-conectadas-y-seguras.html
84 https://womcy.org/

Promoting career pathways

Relevance

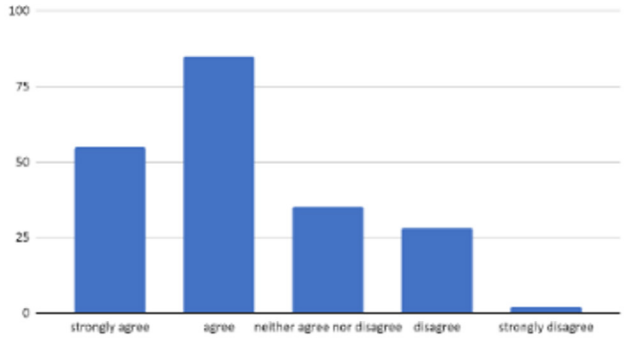
There are many opportunities for workers to start and advance their cybersecurity careers within organizations. Because employees in cybersecurity roles value jobs that allow them to grow and develop, employers who cannot offer generous salaries can still compete for talent by offering career pathways that show growth and learning potential. These frameworks help cybersecurity professionals prepare for key jobs within the organization, for common transition opportunities between them, and for detailed information about the salaries, credentials, and skill sets associated with each cybersecurity role. These frameworks are generally well coordinated sequences of educational and training offerings and support services that help professionals advance their careers in a particular industry or occupation.

Challenges

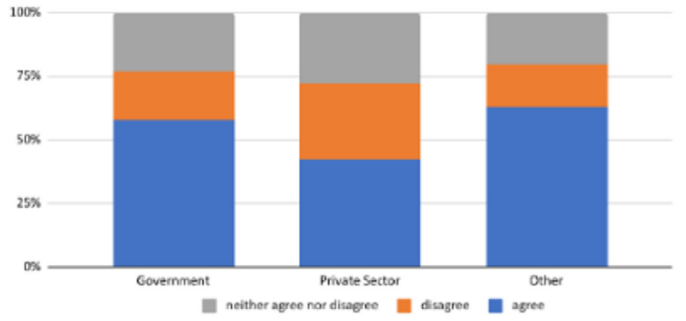
Just over 6 in 10 cyber companies (63%) in the UK report that they employ staff who have or are working toward cybersecurity-related qualifications (i.e., in higher education, apprenticeships, or other certified training) (DCMS & IPSOS, 2022). However, membership fees for some professional associations, as well as fees for some programs in career pathway frameworks, may be higher than the average monthly salary of some cybersecurity professionals in developing countries (GFCE, 2022). Additionally, two-thirds of stakeholders surveyed in a study on the global development of cybersecurity as a profession agreed that cybersecurity career paths are unclear and, of those, the majority thought this lack of clarity discouraged people from joining or remaining in the cybersecurity profession. This opinion was strongest among people working in government (6%) and less strong among people working in the private sector (40%) (GFCE, 2022).

Some figures

Chart 39.
Perceptions of career pathways
To what extent do you agree that career pathways are unclear?



Source: (GFCE, 2022)



Source: (GFCE, 2022)

Good practices

The interactive website *Cyberseek.org*[86] contains several tools designed to help professionals plan career paths that showcase key cybersecurity jobs, common transition opportunities between them, and detailed information on salaries, credentials, and skill sets associated with each role. For example, the *National Initiative for Cybersecurity Careers and Studies* has developed the *Career Pathway Roadmap,*[87] an interactive tool for working professionals (cyber and non-cyber) and employers to explore and build their own career roadmap across the 52 different NICE Framework work roles. Supporting career paths and creating long-term economic and employment value requires retraining programs with a transformational learning approach. Many professional certification providers offer career paths to follow, and each credential represents a different level of expertise. Leading certification providers include (ISC)2 (https://www.isc2.org/), CompTIA (https://www.comptia.org/), ISACA (https://www.isaca.org/), GIAC (https://www.giac.org/), EC-Council (https://www.eccouncil.org/) and SANS (https://www.sans.org/).

85 The certification most frequently requested by cyber employers is *Certified Information Systems Security Professional (CISSP),* found in 39% of online job postings in 2021 that requested a specific certification. The *Cisco Certified Network Professional* and *Cisco Certified Network Associate* certifications were also in high demand in the United Kingdom, with 21% of job postings requesting each one.
86 https://www.cyberseek.org/pathway.html
87 https://niccs.cisa.gov/workforce-development/career-pathway-roadmap

Retaining the workforce

Relevance

Human resources departments within organizations should implement cybersecurity workforce development strategies to meet current and future workforce demands. When there is a shortage of qualified professionals, organizations must innovate to grow their workforce. For companies to protect themselves reliably over the long term, the most important thing they can do is to focus on retaining their best employees. According to the World Economic Forum (WEF, 2022), retention and work/life balance are also factors that amplify the talent shortage. Six percent of cyber leaders say their organizations lack critical people and skills; 6% depend on third parties and external resources; 37% have the people and skills they need today; and 47% have training and skills gaps in some areas. Organizations must improve their ability to retain people by enabling employees to upgrade their skills, become certified, and continue their professional development.

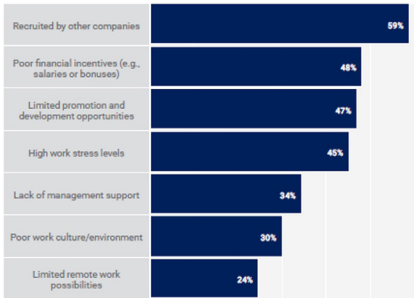
Challenges

Organizations face several challenges in retaining talent in the cybersecurity workforce. The inability to recruit and retain the cybersecurity talent needed to address today's challenges is a key limiting factor for both the private and public sector. There is a dearth of sufficient and appropriate training programs for employees, especially in SMEs. This segment also faces risks due to low-quality cybersecurity training in the external training market, as most organizations purchase training primarily based on cost and speed, without initially recognizing the value of longer courses.[88] Organizations today must prioritize the personal success of employees through professional development (LinkedIn, 2022). According to ISACA, 60% of the survey responses point to the difficulty of retaining talent in cybersecurity companies, the main causes being recruitment by other companies, low incentives, and limited promotion (ISACA, 2022).

Some figures

Chart 40.

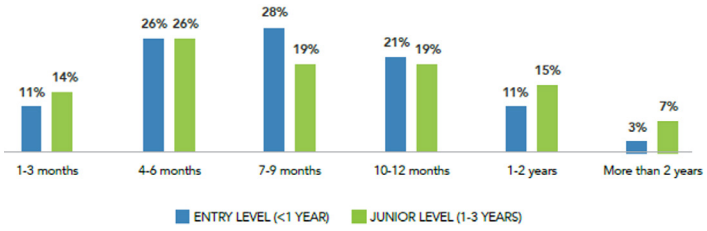
Leading causes of resignation for cybersecurity professionals



Source: (ISACA, 2022)

Chart 41.

How long does it take to train entry-level and junior staff?



Source: (ISC2, 2022b)

Good practices

Organizations should implement innovative strategies to retain their workforce and talent, combining various incentives such as salary, training, reputation, and opportunities for advancement. According to Mercer, organizations should consider different reward structures for different work models (MERCER, 2022). For example, a shift to skills-based pay is one solution. It also mentions that important generational differences must be considered;[89] for example, Gen X and baby boomers most value a sense of belonging, while millennials place greater value on opportunities to learn new skills. Mentoring, certifications, and career guidance are among the tools and resources that study participants offer to help newcomers gain experience, develop their skills, and achieve new career milestones (ISC2, 2022b). Some actions organizations might take to retain the workforce and address the impact of the cybersecurity skills shortage include increasing commitment to training, increasing compensation levels, offering incentives such as paying for certifications and participation in events, and creating/enhancing cybersecurity traineeship programs (ESG, 2021).

88 This encouraged low quality training courses to enter the market, which in turn made it difficult for organizations to distinguish between good and bad training (DCMS & IPSOS, 2022). This report also mentioned that universities and higher education providers had also skewed the market in this direction by favoring externally delivered short courses that had high pass rates. One indicator of this was the wide gap in charges between the cheapest and most expensive training providers.
89 An example of this can be seen in the LinkedIn *Global Talent Trends 2022* report (LinkedIn, 2022), in which 66% of Gen Z respondents to its global survey said they would like to see more investment in mental health and wellness to improve corporate culture, while 51% of millennials, 41% of Gen X, and only 31% of baby boomers supported the idea.

05

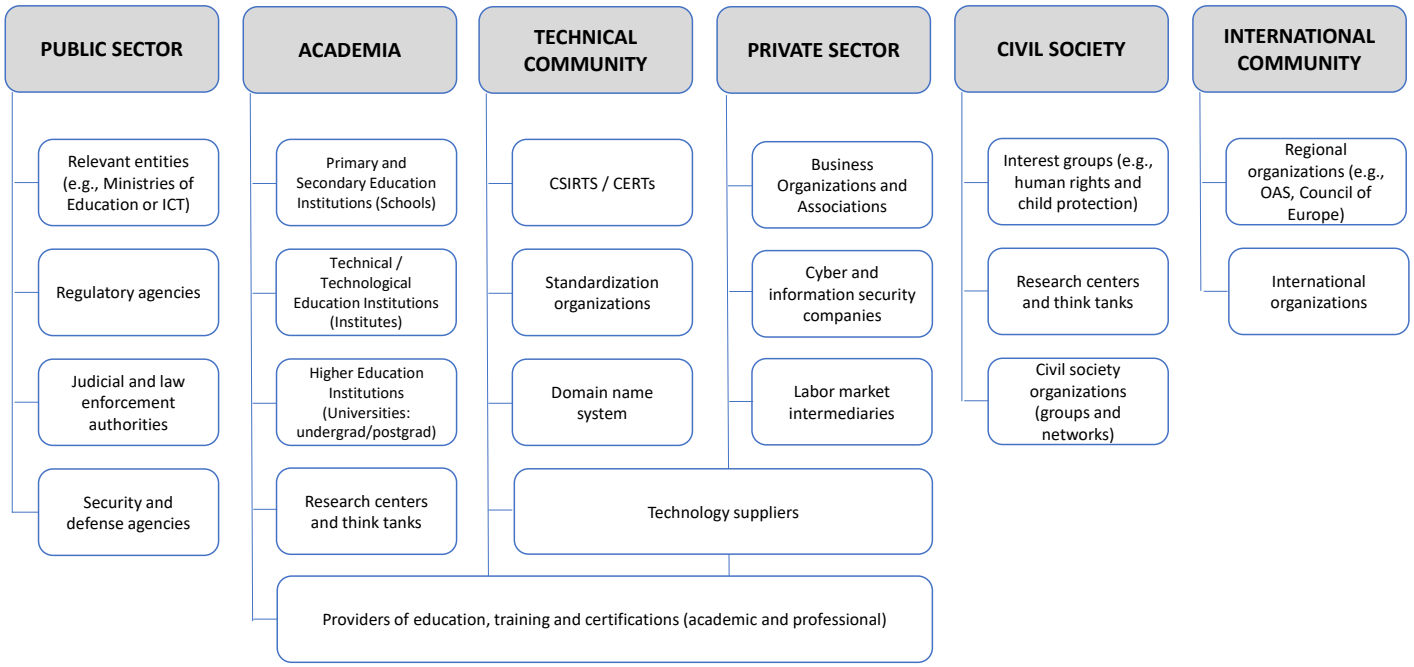
THE REGION'S MULTIPLE STAKEHOLDERS MUST ACT

Given today's cybersecurity labor market conditions and the challenges we have discussed, Latin American and Caribbean countries must develop and implement new educational and training pathways to provide a greater number of cybersecurity job seekers with the necessary skills, and organizations must invest in innovative strategies for recruiting and training the current workforce.

The identified problems associated with the shortage of cybersecurity workers and skills in the region can be addressed by getting multiple stakeholders (public sector, academia, technical community, private sector, civil society, and the international community) to act. Globally, the most common practice for tackling the issue is to comprehensively address the challenges in the cybersecurity labor market through inclusive and cooperative approaches that encourage multi-stakeholder participation in the cybersecurity ecosystem.

Chart 42.

Schematic representation of the multiple stakeholders related to cybersecurity workforce development[90]



Source: Prepared by the authors.

90 This chart illustrates the relevant stakeholder groups, including a non-exhaustive list of potential stakeholders in each group. It is important to recognize that any grouping of stakeholders should be approached with flexibility and caution, as the categories and subcategories may change according to the local context for each country in the region and the self-identification of stakeholders. As a general rule, the framework for identifying relevant stakeholders should be as broad and flexible as needed so that it does not restrict effective stakeholder participation.

5.1. RECOMMENDATIONS FOR THE REGION'S GOVERNMENTS

The shortage of cybersecurity professionals and skills is a multidimensional policy issue involving multiple stakeholders and is compounded by many factors. Governments in the region play a key role in developing the workforce to provide people with education, skills development, and better access to employment and advancement in the labor market to achieve maximum overall sustainable economic growth.

First, governments should develop national strategies and action plans for cybersecurity workforce development, taking at least the following actions:

- Create a governance model for the coordination and harmonization of multiple stakeholders to strengthen the country's capabilities around cybersecurity workforce development.
- From the labor supply side, prepare and include an action plan for cybersecurity education,[91] addressing the challenges identified below.
- From the labor demand side, prepare and include an action plan to promote the recruitment, retention, training, and education of the current cybersecurity workforce, addressing the challenges identified below.
- Fund national strategies and action plans related to cybersecurity workforce development.
- Create skills and employment hubs / funds (possible subsidy programs for specific segments of the population).

Second, governments should establish national and regional leadership and coordination structures, taking at least the following actions:

- Involve all multiple stakeholders in high level decision making and working groups.
- Promote maximum collaboration and cooperation among the multiple stakeholders, considering their roles and responsibility in workforce training and development.
- Promote social dialogue and multi-stakeholder partnerships for the development of workforce skills.
- Facilitate the implementation of joint regional initiatives to address the labor shortage and the cybersecurity skills gap.
- Develop ecosystems for cybersecurity training that motivate students and professionals to pursue careers in cybersecurity.

91 See the proposal developed by the OAS Cybersecurity Program and Amazon Web Services (AWS) called *"Cybersecurity Education: Planning for the Future through Workforce Development"* in Edition 9 of the 2020 White Paper Series (OEA & AWS, 2020)

Third, governments may consider the following points to address specifically identified challenges in developing public-private partnerships, updating legislative and regulatory frameworks, continuously collecting and assessing related data, and raising awareness and disseminating resources, tools, and information for cybersecurity workforce development.

1) Develop strategies for creating public-private partnerships

Cybersecurity workforce development depends on close coordination between governments, the private sector, and education or training providers. In particular, governments should:

- Involve employers in the launching of new training programs.
- Update existing curricula and program delivery to improve work-based learning programs to meet labor market needs.
- Design a comprehensive cybersecurity workforce development strategy that not only covers policies aimed at the education, training, and skills-building system, but also promotes the development of public-private partnerships.

2) Update or adapt legislative and regulatory frameworks to promote workforce development

In their 2020 report on cybersecurity, the OAS and IDB underscore how important it is for countries in the Latin America and Caribbean region to have effective legal and regulatory frameworks for improving cybersecurity maturity (OAS & IDB, 2020). Since a legislative framework establishes the baseline of minimum behavior upon which further cybersecurity capabilities can be built, the goal is for countries to have sufficient legislation in place to harmonize practices at the regional and international levels. Therefore, governments should:

- Bring into line, adapt, and/or harmonize the national legal and regulatory framework with the dynamics of the digital economy and its inherent uncertainties, since these national frameworks are often dispersed and outdated in many areas related to cybersecurity, including aspects related to the challenges identified in the labor market analysis that affect workforce development in the region.

3) Promote the ongoing collection and assessment of labor market and cybersecurity workforce data

Cyber workforce development staff generally lack accurate data to measure and understand the impact of different cybersecurity workforce efforts and policy interventions. Closing gaps in the cybersecurity labor market requires a detailed understanding of the cybersecurity workforce in the countries of the region; therefore, governments in the region should:

- Encourage multi-stakeholder cooperation for information gathering and sharing.[92]

92 In the United States, the CyberSeek initiative introduces local employers, educators, guidance and career counselors, students, current workers, policymakers, and other interested parties to tools such as: (i) an interactive heat map that provides instant and granular status of the supply and demand for cybersecurity jobs at the state and metro area level, (ii) a proposed career pathway showing key cybersecurity jobs, common transition opportunities between them, and detailed information on salaries, credentials, and skill sets associated with each role, and (iii) a tool that provides information on different education and training programs as well as training providers in the country.

- Promote multi-stakeholder collaboration to research and disseminate findings on the factors influencing the impact of cybersecurity education, training, and workforce development.[93]
- Use research findings to inform programs and curriculum design, foster lifelong learning opportunities, have an impact on student success, and ensure equitable access.
- Establish and maintain a directory of programs and project activities, initiatives, and resources related to cybersecurity career awareness, exploration, preparedness, placement, maintenance, and mentoring.
- Promote the analysis of cybersecurity market needs and related trends through the identification of metrics that show the scope of the problem and possible measures to address it.

4) Raise awareness and disseminate resources, tools, and information for cybersecurity workforce development

Countries in the region need to make the general population more aware of their personal security, while also raising awareness of professional opportunities in cybersecurity, which would help set future cybersecurity professionals on track for their careers. Governments should:

- Raise awareness and disseminate cybersecurity workforce development resources, tools, and information to help organizations recruit qualified professionals more efficiently and effectively, and provide this critical workforce with clear job descriptions and development opportunities.
- Adopt and promote the design and development of cybersecurity education databases, especially in the higher education sector, and databases to promote labor demand in both the private and public sectors.
- Working with industry to raise awareness about qualifications, certifications, degrees, and apprenticeship standards, reaching both employers and cybersecurity professionals (GFCE, 2022).

93 The United Kingdom's experience in conducting surveys, studies, and detailed reports on the cybersecurity labor market, which gather data on skills gaps and shortages based on an analysis of the cybersecurity labor supply and demand, is of particular note. Such reports highlight, on the one hand, the challenges that employers face in meeting their hiring and training needs, and on the other, the perspective of individuals entering or active in the cybersecurity labor market, illustrating the difficulties they face in finding the right career and training pathways, as well as the growing need for a holistic skill set in various roles.

5.2. RECOMMENDATIONS ON THE LABOR SUPPLY SIDE

To encourage scientific vocations among children and young people in the region, related public sector entities and academia (primary and secondary education institutions) should:

- Assess and update national educational policies that emphasize STEM skills for teachers and students.
- Encourage digital literacy in the child and youth population by promoting scientific vocations and an emphasis on STEM.
- Organize mass events to tap into the talent pool and invest in developing practices for building STEM skills and capacity.

To strengthen English language proficiency in the region, related public sector entities and academia (primary, secondary, and higher education institutions) should:

- Assess and update current national educational policies for the promotion of languages and bilingualism and identify the key barriers to opportunities for students and teachers to achieve English language proficiency in the region's educational systems.
- Update national bilingualism programs and/or strategies, incorporating the use of new learning technologies.
- Develop complementary educational content in the English language related to cybersecurity risk management and train elementary and middle school students, as well as students in higher education.

To raise awareness and understanding of cybersecurity at an early age, related public sector entities and academia (primary and secondary education institutions) should:

- Identify and share effective practices to promote children and youth awareness and discovery of cybersecurity careers.
- Provide information and tools on cybersecurity-related career options to those who influence career choices (e.g., teachers, school counselors, career coaches, mentors, and parents or guardians).
- Raise awareness of privacy and cybersecurity among technology users, especially young users, through mass training and capacity building exercises.

To promote access to educational opportunities, related public sector entities and academia (technical/technological education and higher education institutions) should:

- Develop and use tools and resources to identify and attract the people most likely to succeed in the labor market.
- Diversify and update elementary, secondary, and higher education curricula to include cybersecurity content.
- Promote and facilitate access to related academic programs.
- Provide more scholarships and more active diversity-focused efforts to increase enrollment.
- Promote and encourage specific subjects such as cryptography in the curricula of elementary, secondary, and higher education.

To connect education with training and industry, the public sector, the private sector, the technical community (standardization organizations), and academia should:

- Promote the use of unified approaches to cybersecurity roles, competencies, skills, and knowledge.
- Develop standardized curricula that introduce a common cybersecurity taxonomy and lexicon for educational institutions to align their curricula to established standards.
- Integrate industry knowledge of cybersecurity into the courses that make up the academic offerings to gradually bridge the disconnect between academia and industry.
- Update cybersecurity education content to apply to both higher learning and relevant industry sectors.
- Promote credible use cases in the academic world for skills development.
- Promote challenges and competitions in the business world for the development of cybersecurity skills.
- Promote a strategy for the certification of cybersecurity degrees at the national level.

To promote access to learning pathways, the public sector, the private sector, and academia, working with *education, training,* and *certification providers* and technology providers should:

- Foster the democratization of knowledge for skills development.
- Ensure clear linkages between schools, universities, industry, and the cybersecurity labor market.
- Increase students' and job applicants' understanding of learning pathways and academic certifications.
- Work to ensure that academic degree programs and industry-recognized certifications effectively measure cybersecurity competencies.
- Increase private sector partner investment in the cybersecurity workforce.

To clarify the definition of cybersecurity profession, the public sector, the private sector, and academia, working with *education, training,* and *certification providers*, technology providers, the technical community (standardization organizations), and the international community should:

- Promote initiatives for national (and if possible, regional) standardization for developing curricula and syllabi to define cybersecurity work under a common language and categorize cybersecurity roles.
- Promote the use of common language and the categorization of cybersecurity roles in the Latin America and the Caribbean region.

5.3. RECOMMENDATIONS ON THE LABOR DEMAND SIDE

To ensure that demand and supply speak a common language, the public sector, the private sector, and academia, working with *education, training,* and *certification providers*, technology providers, the technical community (standardization organizations), and the international community should:

- Develop frameworks for generating a common lexicon and language to create incentives and promote the cybersecurity workforce.
- Provide clarity on functions, roles, and responsibilities for cybersecurity workforce development.
- Use new and emerging technologies to improve connections and matching between employers and job seekers.

To adjust hiring requirements to attract top talent, public sector entities and private sector organizations should:

- Improve capabilities to effectively recruit and hire the talent needed to manage cybersecurity-related risks.
- Promote the establishment of more entry-level positions and opportunities that provide avenues for growth and advancement.
- Foster communication between human resources and cybersecurity departments in order to agree on the profiles required by the organization.

To promote diversity, equity, and inclusion in the workforce, the public sector, the private sector, academia, the technical community, civil society, and the international community should:

- Promote diversity in the workforce at all levels, improve gender balance, and create programs considering the diversification of the workforce.
- Identify and promote effective learning methods, practices, and educational programs that will grow and develop a diverse and inclusive cybersecurity workforce.
- Ensure funding for training, upskilling, and retraining, especially for women, disadvantaged groups, and the most affected sectors.

To promote career pathways, the public sector, the private sector, and academia, working with *education, training,* and *certification providers* and technology providers should:

- Make career pathways in cybersecurity more accessible and affordable.
- Expand budgets in existing cybersecurity workforce development efforts.
- Encourage effective practices to retrain unemployed, underemployed, incumbent workers to prepare them for careers in cybersecurity.
- Take specific measures to encourage the provision of and participation in work-based learning programs, including apprenticeships and traineeships.
- Identify, measure, and disseminate successful cybersecurity work-based learning opportunities.
- Offer incentives, through various mechanisms, for to organizations to develop internal courses and certifications, products, frameworks, etc.

To retain the workforce, public sector entities and private sector organizations should:

- Identify, attract, recruit, and retain the best available talent by implementing innovative training and education strategies, such as: (i) *Upskilling* (processes of learning new skills or teaching new skills to employees), (ii) *Reskilling* (processes of training employees in a completely new skill set to prepare them to take on a different role within the company), and (iii) *New Skilling* (continuous learning processes to help develop high-demand skills, whether an individual is trying to improve current capabilities or needs a complete upgrade to develop entirely new ones).
- Promote work-based learning programs, including apprenticeships and traineeships.
- Provide incentives to convert entry-level employees into mid-career and senior talent.
- Encourage and enable ongoing employee development and training, including rotational and exchange programs, to promote the retention of current talent with diverse skills and experience.

06

REFERENCES

ASPENDIGITAL. (September 2021). Diversity, Equity, and Inclusion in Cybersecurity. Retrieved from https://www.aspeninstitute.org/wp-content/uploads/2021/09/Diversity-Equity-and-Inclusion-in-Cybersecurity_9.921.pdf

CISCO. (2022). *Employees are ready for hybrid work, are you? Cisco Global Hybrid Work Study* 2022. Retrieved from https://www.cisco.com/c/dam/m/en_us/solutions/global-hybrid-work-study/reports/cisco-global-hybrid-work-study-2022.pdf

Computer Science. (2022). Retrieved from Women in Computer Science: Getting Involved in STEM: https://www.computerscience.org/resources/women-in-computer-science/

Cook, I. (September 15, 2021). *"Who Is Driving the Great Resignation?"*. (T. H. Review, Editor) Retrieved from https://hbr.org/2021/09/who-is-driving-the-great-resignation

CSA. (2021). Operational Technology Cybersecurity Competency Framework. Retrieved from https://www.csa.gov.sg/News/Publications/operational-technology-cybersecurity-competency-framework-(otccf)

CSES. (2018). Identifying the Role of Further and Higher Education in Cyber Security Skills Development. Retrieved from https://www.gov.uk/government/publications/the-role-of-further-and-higher-education-in-cyber-security-skills

CyberSeek. (August 2022). *Cybersecurity supply/demand heat map*. Retrieved from https://www.cyberseek.org/heatmap.html

DCMS & IPSOS. (2022). Cyber security skills in the UK labour market 2022 - Findings report. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1072767/Cyber_security_skills_in_the_UK_labour_market_2022_-_findings_report.pdf

DELOITTE. (2020). Workforce development: Equipping the workforce for the future. Retrieved from https://www2.deloitte.com/us/en/pages/human-capital/articles/workforce-development-strategies.html

DNP. (2020). *Política Nacional de Confianza y Seguridad Digital de Colombia* (CONPES Document 3995 of 2020). Retrieved from https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

DNP. (2022). *Política Nacional de Ciencia, Tecnología e Innovación de Colombia* 2022-2031 (CONPES Document 4069 of 2022). Retrieved from https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%c3%b3micos/4069.pdf

EF. (2022). *EF EPI - Índice EF de nivel de inglés*. Retrieved from https://www.ef.com.co/assetscdn/WIBIwq6RdJvcD9bc8RMd/cefcom-epi-site/reports/2022/ef-epi-2022-spanish.pdf?_gl=1*5wznb6*_up*MQ..&gclid=Cj0KCQiA4OybBhCzARIsAIcfn9mz7Nn4piKVx-JYcTR-p1Px287XVTyRjwOn7bOtRsA-DaN2ymmjqQoaAkv6EALw_wcB&gclsrc=aw.ds

ENISA. (2022). European Cybersecurity Skills Framework ECSF - Draft v0.5. Retrieved from https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/ecsf-profiles-v-0-5-draft-release.pdf

ESG. (2021). ESG Infographic: the Life and Times of Cybersecurity Professionals 2021. Retrieved from https://www.esg-global.com/research/esg-infographic-the-life-and-times-of-cybersecurity-professionals-2021

ETHNOLOGUE. (2022). *What are the top 200 most spoken languages?* Retrieved from https://www.ethnologue.com/guides/ethnologue200

FORBES. (July 31, 2022). *The Future Of Work: More Hybrid, More Collaborative, More Automated.* Retrieved from https://www.forbes.com/sites/danielnewman/2022/07/31/the-future-of-work-more-hybrid-more-collaborative-more-automated/?sh=77896d589c46

FORTINET. (August 18, 2022). Retrieved from https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2022/fortinet-registro-137-mil-millones-de-intentos-de-ciberataques-e

FORTINET. (2022). 2022 Cybersecurity Skills Gap - Global Research Report. Retrieved from https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2022-skills-gap-survey.pdf

GFCE. (July 2022). Developing Cyber Security as a Profession - A Report by the Global Forum on Cyber Expertise. Retrieved from https://thegfce.org/wp-content/uploads/2022/08/GFCE-Report-Developing-Cyber-Security-as-a-Profession-July-2022-1.pdf

GFCE. (2022). Pre-University Cyber Security Education: A report on developing cyber skills amongst children and young people. Retrieved from https://thegfce.org/wp-content/uploads/2022/08/GFCE-report-20220731.pdf

GLOBAL PARTNERS DIGITAL. (2018). *Multistakeholder Approaches to National Cybersecurity Strategy Development*. Retrieved from Multistakeholder Approaches to National Cybersecurity Strategy Development: https://www.gp-digital.org/publication/multistakeholder-approaches-to-national-cybersecurity-strategy-development/

IDB. (2020). The Future of Work in Latin America and the Caribbean - What is the impact of automation on employment and wages? Retrieved from https://publications.iadb.org/publications/english/viewer/The-Future-of-Work-in-Latin-America-and-the-Caribbean-What-is-the-Impact-of-Automation-on-Employment-and-Wages.pdf

IDB. (2021). *El impacto de la automatización, más allá de las fronteras*. Retrieved from https://blogs.iadb.org/trabajo/es/el-impacto-de-la-automatizacion-mas-alla-de-las-fronteras/

IDB, ECLAC & KAS. (2021). Post Pandemic Covid-19 Economic Recovery: Enabling Latin America and the Caribbean to Better Harness E-commerce and Digital Trade. Retrieved from https://publications.iadb.org/publications/english/viewer/Post-Pandemic-Covid-19-Economic-Recovery-Enabling-Latin-America-and-the-Caribbean-to-Better-Harness-E-commerce-and-Digital-Trade.pdf

ILO. (August 11, 2022). *Global Employment Trends for Youth.* Retrieved from https://www.ilo.org/global/about-the-ilo/newsroom/news/WCMS_853078/lang—en/index.htm

ILO. (2022). *ILOSTAT*. Retrieved from https://ilostat.ilo.org/es/data/

ISACA. (2022). State of Cybersecurity 2022. Retrieved from https://www.isaca.org/go/state-of-cybersecurity-2022

ISC2. (2021). Cybersecurity Workforce Study. Retrieved from https://www.isc2.org/Research/Workforce-Study

ISC2. (2022a). Cybersecurity Workforce Study. Retrieved from https://www.isc2.org/-/media/2A313135414E400FA0DBD364FD74961F.ashx

ISC2. (2022b). Best Practices for Hiring and Developing Entry and Junior-Level Cybersecurity Practitioners. Retrieved from https://www.isc2.org//-/media/ISC2/Research/2022/ISC2-Cybersecurity-Hiring-Managers-Guide.ashx

Kang, N. (2019). A review of the effect of integrated STEM or STEAM (science, technology, engineering, arts, and mathematics) education in South Korea. *Asia Pac. Sci. Educ*. doi: https://doi.org/10.1186/s41029-019-0034-y

LinkedIn. (2022). The Reinvention of Company Culture - Global Talent Trends 2022. Retrieved from https://business.linkedin.com/content/dam/me/business/en-us/talent-solutions-lodestone/body/pdf/global_talent_trends_2022.pdf

LinkedIn. (2022). The Transformation of L&D - Learning leads the way through the Great Reshuffle. Retrieved from https://learning.linkedin.com/content/dam/me/learning/en-us/pdfs/workplace-learning-report/LinkedIn-Learning_Workplace-Learning-Report-2022-EN.pdf

MERCER. (2022). Rise of the relatable organization - Global Talent Trends 2022 Study. Retrieved from https://www.mercer.com/our-thinking/career/global-talent-hr-trends.html

MichaelPage. (2022). *Estudio de Perspectivas LATAM 2022*. Retrieved from https://www.michaelpage.com.co/estudios-y-tendencias/perspectivas-2022

MICROSOFT. (March 23, 2022). *Closing the cybersecurity skills gap – Microsoft expands efforts to 23 countries*. Retrieved from https://blogs.microsoft.com/blog/2022/03/23/closing-the-cybersecurity-skills-gap-microsoft-expands-efforts-to-23-countries/

MINEDUCACION. (September 2022). *Sistema Nacional de Información de la Educación Superior -SNIES-*. Retrieved from https://hecaa.mineducacion.gov.co/consultaspublicas/programas

NICCS. (2022). *Cyber Career Pathways Tool*. Retrieved from https://niccs.cisa.gov/workforce-development/cyber-career-pathways-tool

OAS & AWS. (2020). Cybersecurity Education - Planning for the Future through Workforce Development. Retrieved from https://www.oas.org/es/sms/cicte/docs/20200925-ESP-White-Paper-Educacion-en-Ciberseguridad.pdf

OAS & GPD. (2022). National Cybersecurity Strategies: Lessons Learned and Reflections from the Americas and Other Regions. Retrieved from https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe

OAS & IDB. (2020). 2020 Cybersecurity Report. Cybersecurity Risks, Progress, and the Way Forward in Latin America and the Caribbean. Retrieved from https://www.gp-digital.org/publication/national-cybersecurity-strategies-lessons-learned-and-reflections-from-the-americas-and-other-regions/

OECD. (2021). OECD Employment Outlook 2021: Navigating the COVID-19 Crissi and Recovery. Paris: OECD Publishing. Retrieved from https://read.oecd-ilibrary.org/employment/oecd-employment-outlook-2021_5a700c4b-en#page1

OECD. (2022). Retrieved from OECD Data - Mathematics performance (PISA): https://data.oecd.org/pisa/mathematics-performance-pisa.htm

OECD. (2022). *Supporting SME development in Latin America and the Caribbean.* Retrieved from https://www.oecd.org/latin-america/regional-programme/productivity/sme-development/

Oxford Martin School. (2022). *Oxford Institute of Populating Ageing.* Retrieved from https://www.oxfordmartin.ox.ac.uk/ageing/

RAND. (2014). Hackers Wanted: An Examination of the Cybersecurity. Retrieved from https://www.rand.org/pubs/research_reports/RR430.html

W3TECHS. (2022). *Usage statistics of content languages for websites.* Retrieved from https://w3techs.com/technologies/overview/content_language

WEF. (2022). Global Cybersecurity Outlook 2022. Retrieved from https://www.weforum.org/reports/global-cybersecurity-outlook-2022/

WEF. (2022). Global Gender Gap Report 2022. Retrieved from https://www.weforum.org/reports/global-gender-gap-report-2022/

WICKR. (February 18, 2021). Obtenido de The Future of Cybersecurity Depends on STEM Education: https://wickr.com/the-future-of-cybersecurity-depends-on-stem-education/

World Bank. (2019). Retrieved from What are the main lessons from the latest results from PISA 2018 for Latin America?: https://blogs.worldbank.org/latinamerica/what-are-the-main-results-pisa-2018-latin-america

WORLD BANK. (2022). *Global Growth to Slow through 2023, Adding to Risk of 'Hard Landing' in Developing Economies.* Retrieved from https://www.worldbank.org/en/news/press-release/2022/01/11/global-recovery-economics-debt-commodity-inequality

2023

Report on
CYBERSECURITY WORKFORCE DEVELOPMENT
in an Era of Talent and Skills Shortages

OAS More rights for more people

Cybersecurity Innovation Councils

CISCO