OECD Skills Studies

Building a Skilled Cyber Security Workforce in Latin America

INSIGHTS FROM CHILE, COLOMBIA AND MEXICO

OECD

OECD Skills Studies

Building a Skilled Cyber Security Workforce in Latin America

INSIGHTS FROM CHILE, COLOMBIA AND MEXICO

OECD
BETTER POLICIES FOR BETTER LIVES

This work is published under the responsibility of the Secretary-General of the OECD. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the Member countries of the OECD.

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Please cite this publication as:
OECD (2023), *Building a Skilled Cyber Security Workforce in Latin America: Insights from Chile, Colombia and Mexico*, OECD Skills Studies, OECD Publishing, Paris, https://doi.org/10.1787/9400ab5c-en.

ISBN 978-92-64-91890-0 (print)
ISBN 978-92-64-43395-3 (pdf)
ISBN 978-92-64-39208-3 (HTML)
ISBN 978-92-64-94663-7 (epub)

OECD Skills Studies
ISSN 2307-8723 (print)
ISSN 2307-8731 (online)

Photo credits: Cover © vs148/Shutterstock.com.

Corrigenda to OECD publications may be found on line at: www.oecd.org/about/publishing/corrigenda.htm.

Foreword

Governments, businesses, and individuals worldwide are facing significant threats from cyber security breaches. In recent years, there has been a substantial increase in the demand for cyber security professionals globally, and this trend is expected to continue, leading to labour shortages in several countries. To address the shortage of skilled workers in the cyber security sector, it is crucial to understand the dynamics of supply and demand for cyber security skills. Governments and organisations can utilise this information to identify weaknesses and determine areas that require additional resources. By analysing job postings, one can identify trends in the demand for cyber security professionals and the skills needed to strengthen organisations' cyber security. Additionally, studying cyber security education and training programmes provides valuable insights into the development of the cyber security workforce and potential discrepancies between supply and demand.

This report analyses the demand for cyber security professionals in Latin America and zooms in on the provision of cyber security education and training programmes in Colombia. The report aims to provide a comparative analysis of cyber security demand in Chile, Colombia and Mexico, with a detailed analysis of the education and training programmes and policies put in place in Colombia to make the profession more attractive and diverse. The report is the second in a series of studies that aim to expand knowledge on the cyber security workforce and related education and training provision in various regions and countries.

This work has been carried out by the OECD Directorate for Employment, Labour and Social Affairs and the OECD Centre for Skills. The report was prepared by Diego Eslava and Annikka Lemmens (Chapters 1 and 2) and Iván Bornacelly (Chapters 1 and 3), under the supervision of Fabio Manca, Viktoria Kis and Marieke Vandeweyer. Editorial assistance was provided by Natalie Corry. Valuable comments were given by Mark Pearson (OECD Deputy Director for Employment, Labour and Social Affairs) and El Iza Mohamedou (Head of the OECD Centre for Skills), as well as by Francesca Borgonovi (OECD Centre for Skills) and colleagues from the OECD Directorate for Science, Technology and Innovation.

The OECD is grateful to stakeholders in Colombia for their input and feedback throughout the project, in particular the Ministry of National Education and Ministry of Information and Communication Technology. Our warm thanks go to the Ministries in the countries analysed that provided feedback to the report and to the many education and training institutions, businesses, research institutions, and other organisations who generously shared their knowledge and insights during bilateral discussions. The support from Microsoft Philanthropies is highly appreciated.

Table of contents

FIGURES

TABLES

Follow OECD Publications on:

https://twitter.com/OECD

https://www.facebook.com/theOECD

https://www.linkedin.com/company/organisation-eco-cooperation-development-organisation-cooperation-developpement-eco/

https://www.youtube.com/user/OECDiLibrary

https://www.oecd.org/newsletters/

Executive summary

Latin America (LATAM) is not immune to the growing global cyber security challenges. The region's quick-paced digital transformation and expanded connectivity make it prone to cyber threats. Both individuals and organisations find themselves increasingly at risk of cyber attacks as they become more reliant on digital technologies for many facets of their daily lives and operations. In addition, Latin America possesses significant assets and essential infrastructure that could represent targets for cyber criminals. Developing a strong cyber security workforce is vital to safeguard the digital assets in the region, uphold economic stability, and protect the privacy and security of its population.

This report analyses the evolution of the demand for cyber security professionals in 2021 and 2022 in Chile, Colombia and Mexico. The analysis leverages data gathered from over 14 million job postings collected from the internet (online job postings, OJPs). The report also explores the supply side, zooming in on the landscape of cyber security education and training programmes in Colombia and the policies and strategies to enhance the accessibility and relevance of these programmes.

In the last decade, Chile, Colombia, and Mexico (like other Latin American countries) have increased their focus on cyber security. These countries have implemented national strategies to enhance safe cyberspace navigation and boost the cyber security sector. This growing attention is mirrored by the sharp rise of online job postings (OJPs) for cyber security professionals between 2021 and 2022, with growth rates significantly outpacing other job categories, particularly in Chile and Mexico. Most of the OJPs in cyber security are situated in major urban areas, the hub of substantial businesses and government entities.

The demand for cyber security professionals is diverse. Cyber security architects and engineers, responsible for designing security solutions, are in high demand, particularly in Chile and Mexico. In Colombia, cyber security analysts, providing essential system security insights, hold the largest share of OJPs. Additionally, Colombia has seen a noticeable surge in demand for cyber security auditors and advisors, pointing to a growing appreciation for assessing security solution efficiency and compliance.

In Chile, Colombia, and Mexico, cyber security OJPs frequently require familiarity with specific frameworks or standards (e.g. ISO 27001) and certain certifications (e.g. Certified Information Systems Security Professional, CISSP). Certifications are crucial to signal candidates' expertise in cyber security, especially as the industry is still in the process of development and evolution. Notably, the most in-demand certifications typically require professionals to have at least five years of experience. However, employers in the region may not always be fully aware of these requirements, which creates a disconnect between the positions that organisations aim to fill and the prerequisites necessary to obtain those certifications. This situation can hinder the hiring process as job seekers may be discouraged from applying, and employers may struggle to find the talent they need among the available candidates.

By evaluating the specific skills and experience needed for entry-level positions, employers can ensure that the skills and certification requirements they set are reasonable for the candidates they seek. In this context, the adoption of cyber security skills frameworks becomes crucial for government, academia and the cyber security industry. These tools create a comprehensive structure of roles and skills that enable organisations to accurately identify the profiles most relevant to their interests. Skills frameworks, therefore, contribute to a better alignment between skills demand and supply, as they bring consistency, relevance, and standardisation to the profession.

The analysis of online job postings also shows that proficiency in English is becoming of paramount importance in the cyber profession in Chile, Colombia and Mexico. According to the analysis, English is among the most relevant transversal skills in cyber security vacancies posted online in the three countries. Moreover, most of the training resources and industry standards are primarily in this language. Boosting English language proficiency is, therefore, key for the available cyber security workforce to stay up to date and overcome obstacles for developing relevant cyber security skills.

Equipping individuals with the right technical and transversal skills is essential to ensure that employers can find the cyber security professionals they need. The Colombian case study presented in this report shows how diverse educational and training routes can prepare for cyber security roles. Colombia's higher education system offers a variety of cyber security training programmes leading to formal qualifications, from vocational to undergraduate courses. The vocational programmes (e.g. technical professional and technologist programmes, lasting 2 and 3 years respectively) provide hands-on training, preparing learners for careers in cyber security operations and management, while undergraduate programmes delve deeper into cyber security theory, fostering research, innovation, and critical thinking. Learners can also acquire basic cyber security skills at lower education levels via integrated modules in technical upper-secondary education.

Besides formal cyber security qualifications, Colombia provides non-formal training opportunities for young people and adults. This type of training is typically shorter and more flexible than traditional educational programmes and often leads to diploma certificates. These certificates, offered predominantly by higher education institutions or specialised training providers, usually require 3 to 12 months to complete and include practical training, case studies, and group discussions. Content varies in complexity and specialisation, from foundational technical knowledge in cyber security to more advanced topics, with some aligned to competency certifications or industry standards. Overall, cyber security programmes yield positive outcomes, with relatively high completion rates and successful transitions into employment or further studies. However, many disadvantaged individuals face multiple barriers (e.g. lack of funding, digital illiteracy, misunderstanding of cyber security roles) when engaging with learning opportunities in the field.

Colombia has implemented various strategies and policies to broaden learning opportunities and diversify its cyber security workforce. Through targeted national strategies, the country has bolstered responses to cyber threats and enhanced its cyber security capabilities. Higher education institutions have increased their flexibility, enabling them to adapt to the changing skill needs in the sector and cater to varied learner demographic. Investments have also been made into the quality of the teaching workforce, with institutions like the National School of Instructors of the National Learning Service (Servicio Nacional de Aprendizaje, SENA) having been vital in addressing ICT teacher shortages, including in the field of cyber security.

Broader initiatives to enhance basic digital skills seek to raise cyber security awareness in the general population and encourage potential learners to develop cyber security technical skills. Policies like "Talento Digital" have been introduced to eliminate financial hurdles that could discourage individuals from exploring these training opportunities. Given the underrepresentation of women in this field, various initiatives have been established by the Colombian Government and other actors to encourage more girls and women to pursue cyber security training and careers.

1 Key insights into cyber security skills in Latin America

This chapter provides an overview of the report's objectives and rationale and summarises the main takeaways. It discusses the results from the analysis of the demand for cyber security professionals in Chile, Colombia and Mexico. It also summarises the main findings from the analysis of the landscape of cyber security education and training programmes in Colombia. It concludes with actionable policy pointers.

The relevance of cyber security skills in a more digitalised and interconnected world

Latin America (LATAM) is not immune to the growing global cyber security challenges. As the region experiences rapid digital transformation and increased connectivity, it becomes more susceptible to cyber threats. The dependence on digital technologies for various aspects of daily life makes individuals and organisations vulnerable to cyber attacks. Furthermore, Latin America is home to valuable assets and critical infrastructure which are potential targets for cyber criminals. Thus, a robust cyber security workforce is crucial to protect the region's digital assets, maintain stability, and ensure the privacy and security of its citizens.

The COVID-19 pandemic has accelerated society's reliance on digital technology, with remote work being rapidly adopted to keep businesses, schools, and other services operational during lockdowns. However, the widespread use of remote work has exposed individuals and firms to unprecedented cyber security threats (World Economic Forum, 2022[1]). With a significant portion of the workforce now working remotely or using hybrid arrangements, cyber criminals are better able to exploit weaknesses in digital security measures.

In this context, cyber resilience[1] has become a crucial societal and policy goal, indicating the need for both private companies and the public sector to anticipate, recover from, and adapt to present and future cyber threats. The World Economic Forum emphasises that for organisations to be resilient, their cyber security teams must be prepared and equipped to face quickly evolving threats, have sufficient budgets, develop and retain talent with adequate cyber security skills (World Economic Forum, 2022[1]). Similarly, the Inter-American Development Bank (IDB) recognises that governments must be equipped to make decisions based on a rapidly changing technological and threat landscape. This requires comprehensive and sustainable cyber security policies, supported by the allocation of financial resources and the development of skilled human capital (IADB & OAS, 2020[2]). The OECD also recommends raising the level of awareness, skills and empowerment across society to manage digital security risk (OECD, 2022[3]). A skilled workforce is, therefore, a cornerstone of cyber resilience, as it enables countries to effectively protect their citizens, organisations, and critical infrastructures.

Against this backdrop, the world is facing a shortage of skilled workforce that hampers the efforts of different actors to achieve cyber resilience. The International Information System Security Certification Consortium, (ISC)^2, estimated a global cyber security workforce gap of 3.4 million people in 2022, an increase of 26% with respect to the 2021 estimation (ISC2, 2022[4]). When turning to Latin America (specifically Mexico and Brazil), (ISC)^2 estimates a cyber security workforce gap of nearly 516 000 people in 2022, although the gap in this region decreased by 26% relative to 2021.

The Organization of American States (OAS) identifies the cyber security gap in Latin America as the short-term consequence of a strong increase in the demand for cyber security professionals that is not met with adequate labour market supply. Several years of training are needed to develop the necessary skills and competencies to be able to work in the sector, which means the gap is not likely to be filled quickly, even though the misalignment in demand and supply has led to significant increases in wages and competition among available skilled cyber workers (Organization of American States and CISCO, 2023[5]). The lack of sufficient training programmes specific to cyber security is one of the reasons limiting the region's ability to build a skilled cyber security workforce (Organization of American States and Global Partners, 2022[6]).

Over the past few years, Chile, Colombia, and Mexico have acknowledged the importance of building capacity to address cyber risk and have implemented cyber security policies (see Box 1.1) including objectives for developing and enhancing skills development in both the private and public sectors (Organization of American States and CISCO, 2023[5]). Recent cyber security policy interventions in these countries have placed them in a relatively good position compared to most countries in the region.

The IADB assesses countries' cyber security readiness against five key dimensions.[2] policy and strategy; cyberculture and society; education, training and skills; regulatory frameworks and standards; and organisations and technologies (IADB & OAS, 2020[2]). According to this assessment, the three countries analysed in this report fall in the mid-level stage of cyber security capacity development. In particular, when focusing on the education, training and skills dimension, the report indicates that the three countries have established and operationalised various education and professional training frameworks and have established opportunities for people to educate in cyber security both at a graduate and undergraduate level.

However, further actions are necessary to deliver tailored training programmes and awareness campaigns to develop cyber security capacity in Chile, Colombia and Mexico. The United Nations Economic Commission for Latin America and the Caribbean (ECLAC) recognises the need for Latin American countries to provide improved training activities and awareness campaigns targeted to SMEs – as this group of enterprises are typically at a disadvantage when facing cyber security challenges (ECLAC, 2022[7]). Additionally, experts have called for greater collaboration between academia, the private sector and national cyber security agencies. By enhancing co-ordination among these key stakeholders in the cyber security sector, it becomes possible to align education, training, and research initiatives with the specific needs and strategic objectives of each country in the evolving cyber security landscape (Ruiz Tagle-Vial and Álvarez-Valenzuela, 2020[8]). Such collaborative efforts will enable the development of a skilled cyber security workforce capable of effectively addressing emerging threats and safeguarding critical digital assets in the region.

Box 1.1. Cyber security policies in Chile, Colombia and Mexico

Faced with accelerated digitisation, which brings increased cyber threats, the governments of Chile, Colombia and Mexico have implemented some ambitious cyber security policies in the last decade (MinTIC, 2020[9]; UNODC, 2017[10]; Government of Mexico, 2017[11]). While earlier cyber security policies focused most on risk management and actively counteracting the increase in cyber threats against the countries, the most recent versions instead focus on citizens' abilities to safely navigate cyberspace and on developing the cyber security industry.

For instance, some of Chile's national cyber security policy goals are to "develop a cyber security culture based on education and good practices […] and to promote the development of a cyber security industry." Colombia's national cyber security policy likewise mentions aiming to "strengthen the digital security capabilities of citizens, the public sector and the private sector to increase the digital confidence in the country". Similarly, Mexico's national cyber security strategy is intended to strengthen cyber security to protect the economy of different sectors of the country and promote technological development and innovation, while boosting the national cyber security industry, in order to contribute to economic development.

These national policies show that the countries recognise the importance of having a population that possesses the skills to operate in cyber space safely, as well as having a skilled cyber security workforce that can work in cyber security roles.

This report: Understanding the demand for and the supply of cyber security skills in a set of Latin American countries

The first crucial step towards addressing the cyber security skills shortage is to grasp what is happening on the supply and demand sides of the labour market. Such knowledge allows businesses and governments to pinpoint their areas of highest weakness and where they need more resources. Job postings serve as valuable data, shedding light on the trending demand for cyber security experts and determining the currently crucial skills to build a sufficiently secure digital organisation. Additionally, examining the offerings of cyber security education and training programmes provides insights into the ongoing development of this specific labour force.

This report marks the second phase of a comprehensive project designed to enhance the understanding of the cyber security workforce and the associated education and training programmes across various regions and countries (see Box 1.2). Each report is divided into two parts, one dedicated to the demand for cyber security professionals and the other to the landscape of cyber security education and training programmes:

- The demand-side analysis leverages big data to scrutinise job postings for cyber security professionals, revealing trends and aspects of employer demand through an examination of both the volume and content of these postings. This second report focuses on the demand for cyber security professionals in three LATAM countries: Chile, Colombia, and Mexico.
- The supply-side analysis focuses on cyber security education and training programmes and the policies and strategies designed to broaden and diversify the cyber security workforce. Each report zooms in on one specific country for this supply-side analysis. For this report, Colombia is the selected country.

Therefore, the goal of this report is to offer a comparative analysis of demand in the three selected countries, providing insights about the development and characteristics of the cyber security profession in the Latin American context. Through the Colombian case study, it provides a deep dive into the kinds of education and training programmes that equip workers for cyber security roles, and the policies that could help to make the profession more appealing and diverse.

Box 1.2. The "Building a skilled cyber security workforce" project

The rationale of the project

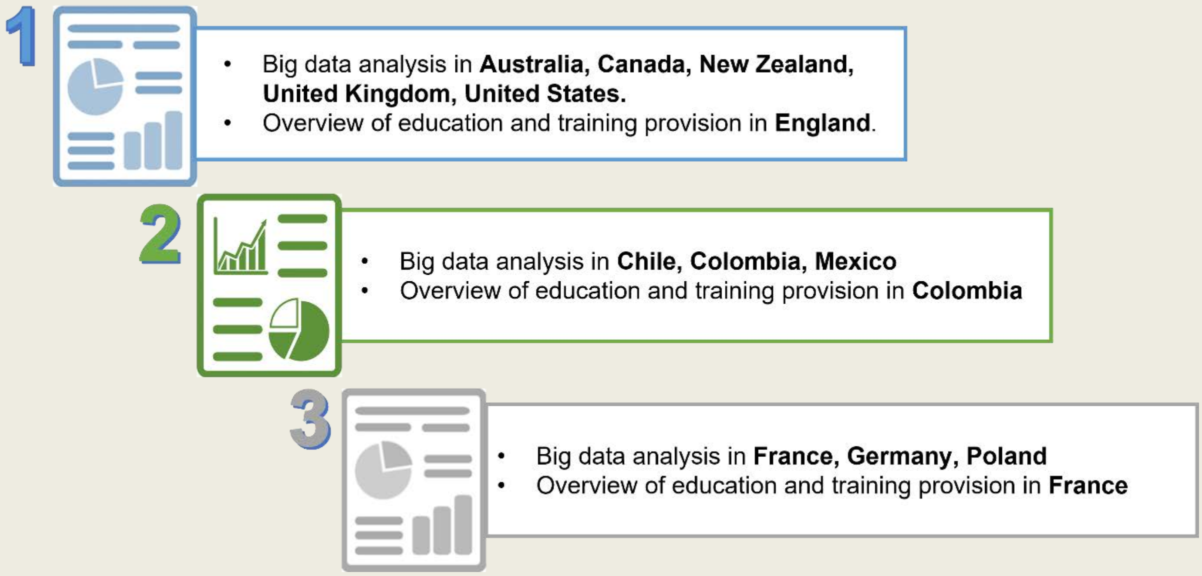
As the demand for cyber security professionals has significantly surged in recent years, and is projected to continue its upward trajectory, labour market shortages have begun to emerge in numerous countries. Given the exorbitant costs associated with cyber threats, it is vital for policy makers and businesses to have timely, detailed insights into both the demand and supply of cyber security-related skills and to learn from global best practices.

This initiative harnesses the broad expertise of the OECD to evaluate the types of cyber security roles that are sought after in worldwide labour markets and to pinpoint the essential skills for establishing a secure digital organisational environment. It also reviews how different countries' education and training systems are cultivating such skills. Additionally, the project promotes an informal forum for dialogue and discussion on best practices and anticipated cyber security skill requirements.

The structure of the project

The project is segmented into three components that blend big data and policy analysis to examine the demand and supply of cyber security skills, as well as the policies and strategies in place to grow and diversify the cyber security workforce, thereby addressing cyber security skill deficits. Each of these three parts zeroes in on different geographical areas (see Figure 1.1), investigating three to five countries for the demand-side analysis and a single country for an in-depth case study on the supply side. This is the second OECD report of three segments that will be synthesised for these analyses. The first report was published in March 2023 (OECD, 2023[12]).

Figure 1.1. Outputs of the cyber security project



- Big data analysis in **Australia, Canada, New Zealand, United Kingdom, United States.**
- Overview of education and training provision in **England**.

- Big data analysis in **Chile, Colombia, Mexico**
- Overview of education and training provision in **Colombia**

- Big data analysis in **France, Germany, Poland**
- Overview of education and training provision in **France**

Methodology

Using big data to understand cyber security skills demand in Latin American countries

Online job postings have become instrumental in tracking labour market developments, playing a pivotal role in providing real-time insights into job demand and industry trends. Traditional labour market data can be limited or outdated, and therefore OJPs offer a dynamic and up-to-date complementary source of information. The increasing reliance on big data in labour market research enables a more nuanced understanding of recent trends and provides insights at a more detailed level compared to traditional data sources. In order to conduct a timely and comprehensive analysis of the demand for cyber security professionals, this report utilises data extracted from nearly 14 million online job advertisements sourced from three selected countries: Chile, Colombia and Mexico.[3]

Specifically, this report uses this dataset to examine the primary trends in the demand for cyber security professionals during 2021 and 2022. To achieve this, it employs text mining and data science techniques to classify job postings within the cyber security domain and extract relevant information from their texts. OJPs enable the analysis of job requirements, such as desired roles and skills, providing valuable insights into the evolving needs of employers in the region. By leveraging the vast amount of data available through online job postings, this report aims to monitor labour market dynamics and identify emerging trends, which can contribute to tailoring policies and training programmes to address the evolving needs of the cyber security workforce in Latin America.

In Latin America, however, informal employment is a challenge for collecting and extracting information from OJPs, as a significant proportion of jobs are not advertised on online employment platforms or though formal labour market channels. Informal employment represents approximately 55-60% of total employment in Colombia and Mexico, while in Chile it is nearly 30% (see Box 1.3). Moreover, even jobs in the formal sector are not always picked up by the OJP data, and this is especially the case for jobs that require low levels of qualifications – which represent a large portion of the labour market in many LATAM countries- as these are more likely to be advertised through other channels (Cammeraat and Squicciarini, 2021[13]). While this can create distortions in the analyses using OJPs, these limitations are likely to be only partly relevant in the current study, as cyber security jobs are more likely to be found in the formal sector and advertised online. Nonetheless, when interpreting data on OJPs for cyber security professionals relative to other parts of the labour market, one should keep these limitations in mind.

Zooming in on strategies for cyber security education and training provision: The case of Colombia

Cyber security education and training programmes take many forms and their content and structure depend on labour market needs and the learners' profiles. Policies and initiatives to expand the supply of cyber security professionals and make the field more accessible also play a major role in shaping the landscape of learning opportunities. To provide insights into how education and training for cyber security roles can be developed, delivered and promoted, this report focuses on one particular country – Colombia. The purpose of presenting a dedicated case study is to provide a detailed description of programmes, policies and initiatives that could serve as inspiration for other countries developing their cyber security education and training sector.

The Colombian case looks at the landscape of cyber security programmes, focusing on professionally-oriented formal education programmes at the undergraduate level or below (e.g. technical professional and technologist programmes) and non-formal programmes (e.g. diploma certificates or *diplomados*). The case study also looks into the efforts put in place to create a strong framework for the provision of cyber security programmes, including national strategies for cyber security skills, and efforts to diversify the provision within higher education and to tackle teacher shortages. Special attention is dedicated to policies that contribute to better access and inclusion, describing challenges and initiatives designed to promote participation in cyber security learning, including among female learners and those from disadvantaged backgrounds. The case study analysis builds on national data and literature, as well as insights gathered from interviews with various key stakeholders in the Colombian education and training sector and cyber security field.

Box 1.3. Labour market informality and the demand for cyber security professionals

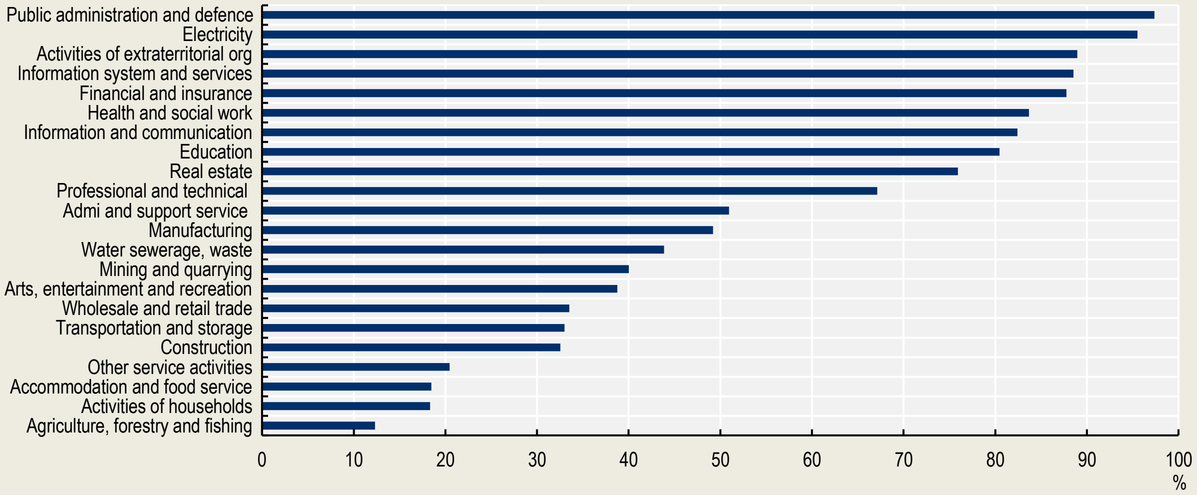
Labour market informality encompasses various aspects that require a comprehensive understanding to address its challenges effectively. In the context of the current analysis, it is important to note that informal employment and economic activities often go unrecorded and undocumented. As a result, official statistics, as well as the analysis in this chapter, may underestimate the actual size and contribution of the informal sector, leading to inaccuracies in measuring demand for labour.

Labour market informality remains a significant challenge in LATAM. According to recent data, an alarming proportion of the population in the region (nearly 70%) live in a house where at least one member has an informal job[4] (OECD et al., 2021[14]). Informality emerged as a response to structural economic challenges, limited job opportunities, and inadequate social protection systems.

While informality is pervasive throughout Latin America, there are notable variations in rates among countries. Countries like Bolivia, Peru and Paraguay have particularly high levels of labour informality, with 70-80% of their workforce operating informal conditions[5] (ILOSTAT, 2023[15]). In the countries analysed in this report, some 55-60% of the working population in Colombia and Mexico are in informal jobs, while in Chile it is nearly 30% (ILOSTAT, 2023[15]). These variations can be attributed to a combination of economic, social, and institutional factors that shape each country's labour market.

When examining the demand for cyber security professionals through the lenses of OJPs, the measurement challenges related to informality are, however, likely to lead to minor biases. Firstly, job advertisements for cyber security professionals are likely to predominantly originate from formal organisations and enterprises that adhere to established recruitment processes. These postings are associated with formal job contracts, legal frameworks, and regulated working conditions. As a result, cyber security professionals are more often sought after in sectors characterised by low levels of informality, such as public administration and defence, information system and services, and financial and insurance (see, for instance, Figure 1.2).

Figure 1.2. Percentage of formal workers by sector in Colombia, 2022



Note: Information system and services includes cyber security sector. The National Statistics Office in Colombia (DANE) follows a definition of informality based on ILO's recommendations, which considers informal employees as those whose employment relationship is not subject to national legal arrangements (for more detail see DANE (2023[16]) and ILO (2003[17])). Variables RAMA2D_4R was used to identify information system and services (Code 62). RAMA2D_4R is based on the Colombian adaptation of International Standard Industrial Classification (ISIC) https://www.dane.gov.co/files/sen/nomenclatura/ciiu/CIIU_Rev_4_AC2022.pdf.
Source: Note: OECD calculations using Gran Encuesta Integrada de Hogares – GEIH and the module of Training for employment.

Secondly, the cyber security field typically places a strong emphasis on professional credentials and qualifications (as discussed in Chapter 2). Skill certifications from national or industry authorities provide workers with means of effectively documenting relevant skills and developing a career path, easing pathways towards formal employment (ILO, 2015[18]). Therefore, this emphasis on professional requirements is likely associated with a higher proportion of formal employment arrangements in the cyber security profession.

Furthermore, organisations operating in sensitive industries, including finance, healthcare, and technology, often face legal obligations and regulatory compliance requirements. These obligations necessitate the formal employment of cyber security professionals, leading to greater adherence to formal procedures and the maintenance of a formal workforce.

In conclusion, while it is important to acknowledge that informality is a challenge when measuring labour market demand, there is limited concern for such biases within the cyber security field. However, results in this report still need to be interpreted with caution given the typically small sample sizes in countries where the informal sector is very large.

Main findings and policy pointers

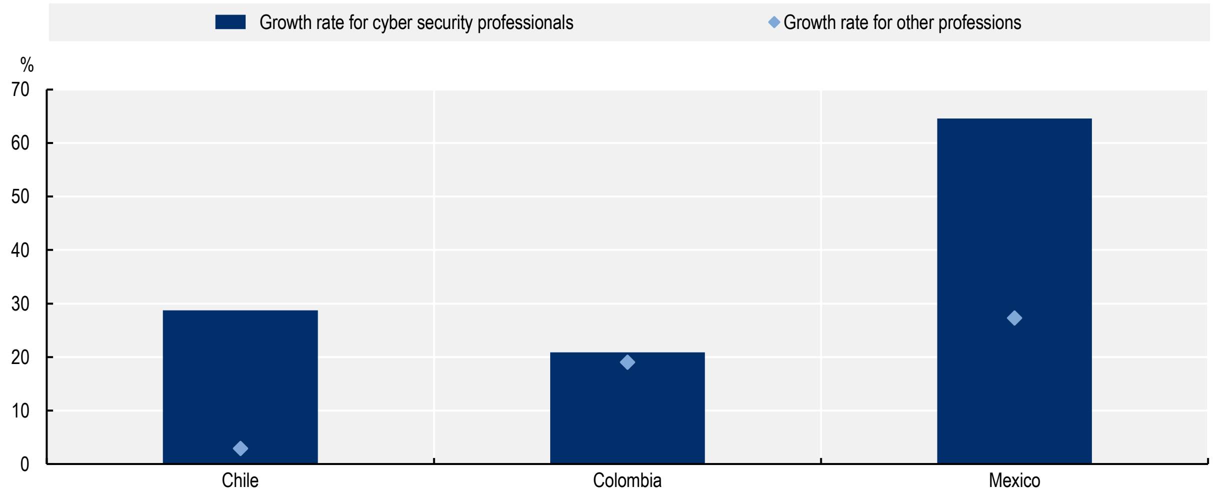
The demand for cyber security professionals is on the rise in Latin America

Chile, Colombia and Mexico have increased their focus on cyber security over the last decade. These countries have designated national cyber security policies and strategies. These formulate goals that, amongst others, aim to improve citizens' ability to safely operate in cyberspace and to boost the cyber security sector in each respective country. In accordance with the rising importance of cyber security in Latin America, the demand for cyber security professionals (approximated by the number of online job postings, OJPs) has increased sharply between 2021 and 2022, with the growth rates for cyber security OJPs significantly outpacing those for other occupations, particularly in Chile and Mexico (Figure 1.3).

Most of the OJPs in the cyber security job market are for jobs in main metropolitan cities where major enterprises and government headquarters are found. The share of cyber security roles posted in metropolitan cities is far larger than the share of the Chilean, Colombian and Mexican populations that live in these areas. What contributes to this finding is that certain industries, such as finance, technology, and professional services, tend to have a higher presence in metropolitan areas due to the availability of skilled labour, infrastructure, and market demand. This boosts the demand for high-skilled positions such as cyber security roles.

Results also show that the demand for cyber security professionals is heterogeneous. Among different job roles, cyber security architects and engineers (those in charge of designing and modelling security solutions) stand at the core of the demand for cyber security professionals, recording the highest share of cyber security OJPs in Chile and Mexico in the period analysed. Cyber security analysts, which provide insights to support planning, operations and maintenance of systems security, represent the largest share of OJPs in the cyber security landscape in Colombia. Furthermore, Colombia experienced a significant increase in demand for cyber security auditors and advisors, indicating a growing recognition of the importance of assessing the efficiency and compliance of security solutions.

Figure 1.3. Growth in online job postings between 2021 and 2022



Source: OECD calculations based on Lightcast data.

In the three LATAM countries under exam in this report, vacancies for cyber security roles frequently specify the need for candidates to possess familiarity with cyber security frameworks or standards, and to have obtained specific certifications. Typically, certifications serve as a standardised measure of candidates' expertise and aptitude in highly specialised areas including, for instance, cyber security. Particularly in Latin America, where the cyber security industry is still developing and rapidly evolving, the signalling function of these certifications is important as employers use them to select qualified candidates, while job seekers employ them to signal their skills.

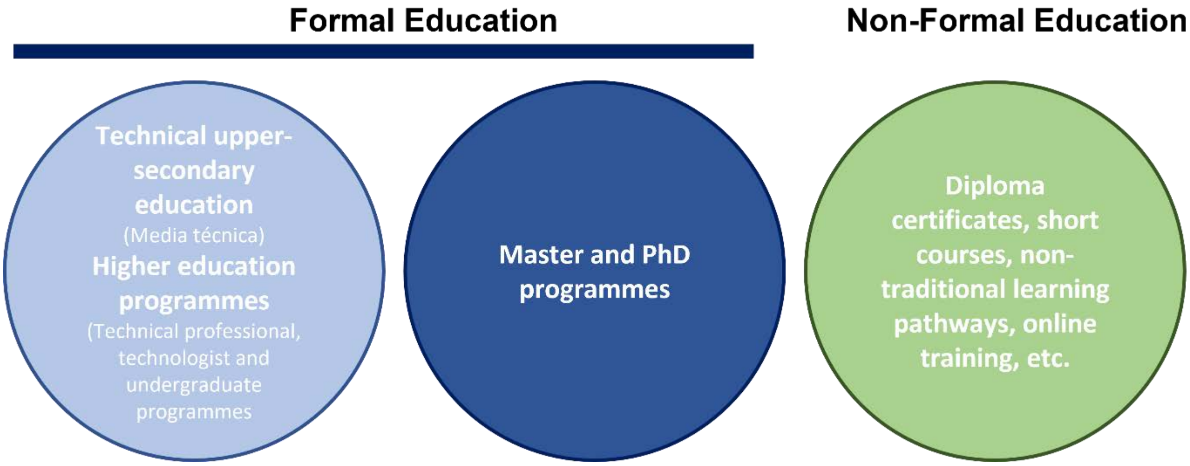
However, it is worth noting that the certifications which are most sought after in Mexico and Colombia are primarily aimed at experienced professionals, as they necessitate a minimum of five years of relevant work experience but, simultaneously, many employers require them in vacancies for entry-level positions. This disparity between job level and certification requirements hampers efficient talent matching in the region's cyber security workforce. Potential employees with the necessary skills may be deterred by these certification needs, while employers struggle to find suitable candidates, resulting in prolonged job vacancies and talent shortages. Consequently, there exists a misalignment between the skill requirements of the labour market and the available job opportunities.

Results also show other important bottlenecks in the ability of the available workforce to match the current demand. For instance, proficiency in English is among the most in demand skill requirements across OJPs for cyber security professionals in the region, but the workforce in LATAM traditionally struggles in this area.

The provision of cyber security education and training programmes in Colombia is diverse

On the supply side, the case study for Colombia shows that there can be various educational and training pathways into cyber security roles, with opportunities for progression (see Figure 1.4). The Colombian higher education system provides multiple cyber security training programmes that lead to formal qualifications recognised by the National Ministry of Education (MEN), including vocational and undergraduate programmes. The former include professional technical and technologist courses focused on practice-oriented training, preparing learners for careers in cyber security operations and management. These programmes take between two and three years to complete. Undergraduate programmes delve deeper into the theoretical foundations and advanced concepts of cyber security, emphasising research, innovation, and critical thinking. Learners can also develop basic cyber security skills at lower levels of education, including through cyber security modules integrated into technical upper-secondary education.

Figure 1.4. Cyber security education and training programmes take many forms in Colombia


Formal Education
Non-Formal Education
Technical upper-secondary education
(Media técnica)
Higher education programmes
(Technical professional, technologist and undergraduate programmes
Master and PhD programmes
Diploma certificates, short courses, non-traditional learning pathways, online training, etc.

Note: Formal education, which leads to formal qualifications such as technical professional programmes, includes courses and programmes offered by universities, technological, professional and technical institutions. For this study, programmes at the Master's level and above are excluded from the analysis. Non-formal education and training include courses outside the formal education system and not leading to formal qualifications (but awarding certificates in some cases), such as diploma certificates.

In addition to these formal cyber security qualifications, young people and adults in Colombia have the opportunity to engage in non-formal training. This type of training, often shorter and more adaptable than programmes within the formal education system, is frequently embodied in the form of diploma certificates. These are predominantly offered by public and private higher education institutions or training providers in the cyber security field. Such flexible courses typically take between three to 12 months to complete, incorporating practical training, case studies, and group discussions. The content of cyber security diploma certificates can vary, both in terms of difficulty and specialisation. Diploma certificates that cover more general concepts furnish students with foundational technical knowledge in cyber security and computer security management. Others address more advanced and complex topics, with some even aligning with competency certifications or industry-required standards.

Colombia has enacted various policies and strategies to broaden learning opportunities and diversify the workforce in the cyber security sector. The country has focused on developing national strategies that strengthen the response to cyber threats and enhance cyber security capabilities, which have been translated into expanding learning opportunities in the field. Increasing flexibility, particularly within higher education institutions, has been one avenue for effectively and rapidly responding to the evolving skill needs in the sector and catering to a diverse group of learners. Training providers have also implemented innovative strategies to address teacher shortages in ICT. To diversify the workforce of cyber security professionals, the country has emphasised the development of basic digital skills across the wider population in an effort to raise cyber security awareness and foster interest among potential learners in pursuing training in this field. Additionally, multiple policies have been implemented to eliminate barriers that might deter interested individuals from exploring these learning opportunities such as providing financial support to engage with basic technical cyber security training. Box 1.4 provides examples of relevant practices in Colombia, which are further documented in Chapter 3.

Policy pointers for building a skilled cyber security workforce

The insights derived from the analysis of the demand for cyber security professionals in Chile, Colombia and Mexico and the detailed analysis of the cyber security education and training in Colombia underscore diverse opportunities for Latin American countries to tackle labour and skills shortages in the sector. This section signals some of them.

Providing structured and comprehensive information on cyber security roles and skills

- The cyber security profession is in constant redefinition, which poses challenges to employers, education and training providers, and learners to understand the different cyber security roles and associated skill requirements. This challenge calls for joint efforts from different actors to develop a structured and comprehensive characterisation of the profession. The adoption of cyber security skills strategies can facilitate the understanding of the cyber security profession in Colombia, as well as in the rest of LATAM, and establish a common taxonomy that contributes to understanding and analysing labour market dynamics in the field. Developing cyber security skills strategies also enhances the design and implementation of policies to overcome labour shortage in the field by providing a roadmap on how to expand the supply of learning opportunities and make training more responsive to employers' needs.
- While knowledge of specific cyber security frameworks is currently in high demand (e.g. ISO/IEC 27000 and ITIL), it is crucial to understand that the field is dynamic and continually evolving, necessitating targeted training efforts to respond to the most recent needs. Assessing and anticipating skills needs through timely and granular data analysis allows countries to generate information about the current and future needs of the cyber security sector (OECD, 2016[19]). These skills assessment and anticipation exercises are vital to stay abreast of emerging trends and to adjust training systems accordingly.
- It is necessary to raise awareness among stakeholders about the importance of a qualified cyber security workforce to respond to cyber risk. Adherence to cyber security frameworks/standards provides essential guidance, best practices, and a common language for organisations and professionals. These tools enable them to establish comprehensive cyber security strategies, mitigate digital security risk, and enhance overall cyber security resilience.

Overcoming barriers to expand and improve the provision of cyber security programmes

- Higher education institutions offer a wide range of formal programmes (e.g. technical professionals, technologists and undergraduates) that lead to entry-level job opportunities in cyber security. Some education institutions also have articulation arrangements (i.e. propaedeutic cycle) which play a crucial role in smoothing the transition from general ICT technical programmes to technologists and undergraduate programmes in cyber security. This approach is designed to prepare students for more specialised studies in their chosen field, building on the solid foundation in core ICT concepts and principles they already acquired.
- Education institutions are increasingly aware of the need to provide programmes and courses that meet the diverse needs of learners, while addressing labour market needs. Diversifying the cyber security offer in higher education to include non-formal training programmes contributes to meeting skills demand more swiftly. It is also essential to facilitate the creation of flexible training programmes that provide sufficient opportunities for cyber security training aligned with labour market needs, that are quality assured and easily accessible, especially for more disadvantaged learners such as those facing financial barriers and digital illiteracy. Such non-formal programmes should ideally lead to certificates that are easily recognised by employers.

- Partnerships between higher education institutions and private sector companies or specialised international training providers are key to expand the provision of cyber security training. In Colombia, this collaboration has led to an expansion of customised short training programmes, such as diploma certificates. This responds to particular skill needs, while typically also being part of learning pathways or building blocks for developing more advanced and specialised skills. Some are even linked to industry certifications which are in high demand in the cyber security sector.
- Teacher shortages affect the provision of cyber security education and training in countries like Colombia. Educational institutions need strategies to attract and retain instructors and professors in ICT fields in a context of significant shortages of cyber-related professionals. Strengthening relationships with companies to provide training to ICT teachers, allowing professionals in industry to dedicate some time to teaching and improving teachers' English proficiency can contribute to reducing shortages.

Tackling digital literacy and language barriers, and raising the interest of potential learners

- Participation in cyber security education and training requires individuals to possess solid basic digital skills. Digital illiteracy is common in Latin America, especially among individuals from disadvantaged backgrounds. In Colombia, for instance, the provision of training programmes covering key fundamentals ICT subjects has been crucial to equip learners with basic concepts for digital navigation and facilitate progression to advanced training. Additionally, developing such skills from a young age can contribute to generating interest in ICT professions, such as in cyber security.
- Enhancing English language proficiency is crucial in mitigating the workforce cyber security gap in LATAM. The English proficiency gap creates significant obstacles to cultivating cyber security skills, as most of the training resources are not available in Spanish. Potential solutions could include offering cyber security training in local languages or providing translation services. Nonetheless, strategies should also focus on improving English proficiency levels in the region to ensure that individuals can access cyber security opportunities offered in English.
- Gender stereotypes can hinder participation in cyber security education and training. Even though countries like Colombia have experienced reductions in the performance gap between boys and girls in mathematics and sciences, the proportion of female professionals in ICT remains low. Latin American countries need initiatives to encourage women to engage in education and training in STEM fields and specifically in ICT and cyber security topics. Platforms and spaces for women to connect, learn and share their experiences in these fields are valuable initiatives towards promoting interest in the profession.

Box 1.4. Relevant practices from Colombia

Colombia has launched a number of interesting initiatives and strategies aimed at enlarging and diversifying the cyber security workforce. These efforts focus on bolstering the availability and quality of cyber security education and training programmes, as well as providing clear information and enticing incentives to foster engagement in the field. A few of these noteworthy practices include:

- **Policy frameworks in cyber security,** such as the most recent document of National Council for Economic and Social Policy (Consejo Nacional de Política Económica Social, CONPES) 3995 on National policy of trust and digital security (DNP, 2020[20]) have been crucial to enhance the digital skills of the workforce, including the introduction of incentives to boost ICT training participation among various target groups (e.g. financial support for disadvantaged individuals to engage with non-formal and formal education) and promoting cyber security education in higher education institutions.
- **Diploma certificates** are offered by higher education institutions, professional associations, and private organisations. Some educational institutions form partnerships with private sector companies or specialised international providers to deliver these certificates. In cyber security, for instance, SENA developed the 'Technological centre of excellence and simulation in cyber security' jointly with MNEMO (an IT and cyber security services company) to deliver diploma certificates in information security and courses related to the field (SENA, 2022[21]).
- **Universities and employers designing short training programmes in cyber security** has become a common practice (for diploma certificates and other non-formal programmes). These short trainings include modules for developing basic technical ICT skills. In some cases, the courses contain modules fully customised by employers to meet their specific needs. These programmes also tend to be flexible and adaptable to students' learning needs, with some including mentoring, tutoring and other types of individual support.
- **Cyber security skills programmes for managers** (MinTIC, 2022[22]) fund training for employees in enterprises to raise awareness of cyber security issues, covering 100% of training expenses. The programmes include two diploma certificate courses for directors and high-level managers and IT managers to promote a culture of cyber security and improve the ability of companies to protect themselves against digital risks and threats.
- **The National school of instructors (ENI)** (SENA, 2023[23]) delivers targeted training for the teaching of ICT, including cyber security programmes. This process includes selecting qualified individuals from industry and developing their pedagogical abilities. Technical training in cyber security is also provided to ensure up-to-date knowledge among ICT teachers.
- **Hacker girls** (MinTIC, 2023[24]) is a national programme that aims at promoting women's participation in technology and cyber security. The programme provides opportunities for women of all ages to develop knowledge and skills in these fields and to encourage more women to pursue careers in technology and cyber security (e.g. hackathons and competitions).
- The **"Por TIC Mujer"** (MinTIC, 2023[25]) programme is an initiative in Colombia launched by the Ministry of Information and Communication Technology (Ministerio de las Tecnologias de la Información y las Comunicaciones, MinTIC) to enhance women's access to and usage of ICTs. The programme aims at overcoming digital illiteracy, improving women's access to technology, and supporting women's use of ICTs for entrepreneurship.

References

Cammeraat, E. and M. Squicciarini (2021), “Burning Glass Technologies’ data use in policy-relevant analysis: An occupation-level assessment”*, OECD Science, Technology and Industry Working Papers*, No. 2021/05, OECD Publishing, Paris, https://doi.org/10.1787/cd75c3e7-en. [13]

DANE (2023), *Empleo informal y seguridad social*, https://www.dane.gov.co/index.php/estadisticas-por-tema/mercado-laboral/empleo-informal-y-seguridad-social. [16]

DNP (2020), *Política Nacional de Confianza y Seguridad Digital (National Policy of trust and digital security)*, https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf. [20]

ECLAC (2022), *A digital path for sustainable development in Latin America and the Caribbean*, Economic Commission for Latin America and the Caribbean, https://conferenciaelac.cepal.org/8/en/documents/digital-path-sustainable-development-latin-america-and-caribbean (accessed on 11 September 2023). [7]

Government of Mexico (2017), *National Cyber Security Strategy*, https://www.gob.mx/cms/uploads/attachment/file/399655/ENCS.ENG.final.pdf (accessed on May 2023). [11]

IADB & OAS (2020), *Cybersecurity: Risks, progress, and the way forward in Latin America and the Caribbean*, https://doi.org/10.18235/0002513 (accessed on April 2023). [2]

ILO (2015), *Promoting transition to formality*, https://www.ilo.org/global/topics/skills-knowledge-and-employability/treepedia/post-training/formality/lang--en/index.htm (accessed on June 2023). (accessed on 2023). [18]

ILO (2003), *Guidelines concerning a statistical definition of informal employment*, http://ttps://www.ilo.org/wcmsp5/groups/public/---dgreports/---stat/documents/normativeinstrument/wcms_087622.pdf (accessed on 1 June 2023). [17]

ILOSTAT (2023), *Statistics on the informal economy*, https://ilostat.ilo.org/topics/informality/. [15]

ISC2 (2022), *ISC2 Cybersecurity Workforce Study*, https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx. [4]

MinTIC (2023), *Hacker Girls*, https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Iniciativas/Hacker-Girls/. [24]

MinTIC (2023), *Por TIC Mujer*, https://formacionapropiacion.mintic.gov.co/course/index.php?categoryid=6. [25]

MinTIC (2022), *Habilidad digitales en ciberseguridad*, https://talentodigital.mintic.gov.co/734/w3-channel.html. [22]

MinTIC (2020), *CONPES 3995 - Política nacional de confianza y seguridad digital*, https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf (accessed on June 2023). [9]

OECD (2023), *Building a Skilled Cyber Security Workforce in Five Countries: Insights from Australia, Canada, New Zealand, United Kingdom, and United States*, OECD Skills Studies, OECD Publishing, Paris, https://doi.org/10.1787/5fd44e6c-en. [12]

OECD (2022), *Recommendation of the Council on National Digital Security Strategies*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0480 (accessed on August 2023). [3]

OECD (2016), *Getting Skills Right: Assessing and Anticipating Changing Skill Needs*, Getting Skills Right, OECD Publishing, Paris, https://doi.org/10.1787/9789264252073-en. [19]

OECD et al. (2021), *Latin American Economic Outlook 2021: Working Together for a Better Recovery*, OECD Publishing, Paris, https://doi.org/10.1787/5fedabe5-en. [14]

OECD/ILO (2019), *Tackling Vulnerability in the Informal Economy*, Development Centre Studies, OECD Publishing, Paris, https://doi.org/10.1787/939b7bcd-en. [26]

Organization of American States and CISCO (2023), *Reporte sobre el desarrollo de la fuerza laboral de ciberseguridad en una era de escasez de talento y habilidades*, https://www.oas.org/es/sms/cicte/docs/Reporte_sobre_el_desarrollo_de_la_fuerza_laboral_de_ciberseguridad_en_una_era_de_escasez_de_talento_y_habilidades.pdf (accessed on 25 April 2023). [5]

Organization of American States and Global Partners (2022), *National Cybersecurity Strategies: Lessons Learned and Reflections from the Americas and Other Regions*, https://www.gp-digital.org/publication/national-cybersecurity-strategies-lessons-learned-and-reflections-from-the-americas-and-other-regions/. [6]

Ruiz Tagle-Vial, P. and D. Álvarez-Valenzuela (2020), *Building Cybersecurity Capacity: Challenges for Post-Secondary Education in Latin America and the Caribbean*, University of Chile, https://doi.org/10.18235/0002513. [8]

SENA (2023), *Escuela Nacional de Instructores “Rodolfo Martínez Tono”*, https://www.sena.edu.co/es-co/comunidades/instructores/Paginas/default.aspx. [23]

SENA (2022), *Sena y MNEMO inauguran en Colombia el primer centro tecnológico de excelencia y simulación en ciberseguridad de América Latina*, https://www.mnemo.com/sena-mnemo-ciberseguridad/. [21]

UNODC (2017), *Chile’s National Cybersecurity Policy 2017-2022*, https://www.unodc.org/e4j/data/_university_uni_/chiles_national_cybersecurity_policy_2017-2022.html?lng=en (accessed on May 2023). [10]

World Economic Forum (2022), *Global Cybersecurity Outlook 2022*, https://www.weforum.org/reports/global-cybersecurity-outlook-2022/. [1]

Notes

[1] The World Economic Forum defines cyber resilience in the *Global Cyber Security Outlook 2022* as “the ability of an organisation to transcend (anticipate, withstand, recover from, and adapt to) any stresses, failures, hazards and threats to its cyber resources within the organisation and its ecosystem, such that the organisation can confidently pursue its mission, enable its culture and maintain its desired way of operating” (World Economic Forum, 2022[1]).

[2] The IADB and OAS study uses the Cyber security Capacity Maturity Model for Nation (CMM) developed by the Global Cyber Security Capacity Centre of the University of Oxford to assess the maturity of the countries’ cyber security capacity (IADB & OAS, 2020[2]).

[3] Data is provided by Lightcast.io.

[4] In this report, informal employment “…refers to working arrangements that are de facto or de jure not subject to national labour legislation, income taxation or entitlement to social protection or certain other employment benefits (advance notice of dismissal, severance pay, paid annual or sick leave, etc.).” (OECD/ILO, 2019[26]).

[5] This figure follows the International Labour Organization (ILO) definition of employment and labour informality: “Employment comprises all persons of working age who, during a specified brief period, were either in paid employment (whether at work or with a job but not at work) or in self-employment (whether at work or with an enterprise but not at work). Informal employment comprises persons who in their main or secondary jobs were: (a) own-account workers, employers and members of producers´ co-operatives employed in their own informal sector enterprises; (b) own-account workers engaged in the production of goods exclusively for own final use by their household (e.g. subsistence farming); (c) contributing family workers, regardless of whether they work in formal or informal sector enterprises; or (d) employees holding informal jobs, whether employed by formal sector enterprises, informal sector enterprises, or as paid domestic workers by households” (ILOSTAT, 2023[15]).

2 The demand for cyber security professionals in Latin America

This chapter provides an analysis of millions of online job postings the describe the demand for cyber security professionals in Chile, Colombia and Mexico in 2021 and 2022. The chapter discusses the demand for different cyber security roles, and the geographical location of the demand. To provide a broader context, it also investigates the demand for digital, engineering, and math-related occupations and explores their correlation with the need for cyber security personnel. Moreover, the research highlights specific skills and certifications that are in high demand within the cyber security professions.

Introduction: Characterising the demand for cyber security skills

In line with global trends, organisations in Latin America are becoming increasingly dependent on digital technologies for their activities. Along with the benefits derived from a digital and interconnected economy, organisations also face increasing challenges to protect their networks and data, as they are now more susceptible to cyber attacks than ever. Successfully anticipating and dealing with cyber security threats requires a skilled cyber security workforce that is able to identify and analyse potential threats and design cyber security responses adapted to businesses' needs.

Within this context, there is increasing evidence of a shortage of trained workers in the cyber security sector across the world. In Latin America, (ISC)^2 estimates a cyber security workforce gap in Mexico and Brazil of nearly 516 000 people in 2022, with 260 000 of those vacancies being located in Mexico ((ISC)2, 2022[1]). This means that the shortage of cyber security personnel in Mexico is second only to the shortage in the United States ((ISC)2, 2022[1]). Fortinet (2023[2]) indicates that 41% of organisations surveyed in LATAM struggle to fill cloud security roles in 2022. These shortages, as well as reliance on foreign expertise, can potentially contribute to organisations' cyber security weaknesses.

Developing cyber security capacity in Latin America is, therefore, a cornerstone of cyber-resilient organisations. However, to accomplish this objective, timely and detailed information is required to shed light on the evolving skill demands in the rapidly changing cyber security landscape. Different data sources can provide valuable insights into the skills required in the cyber security sector. For instance, experts have signalled the opportunities of using the information on cyber attacks collected by national Cyber Security Incident Response Teams (CSIRT) to promote research and skills development in relevant areas for each country (Ruiz Tagle-Vial and Álvarez-Valenzuela, 2020[3]). However, progress on how to best use this data has been limited.

An additional rich source of information that is available to analyse the evolution of labour and skill demands in cyber security is that reliant on the collection of online job postings (henceforth, OJPs). This type of data offers many advantages over traditional data sources such as labour force surveys or national accounts data and they can provide a detailed characterisation of the demand in the Latin American cyber security labour markets. On the one hand, OJPs provide timely data on emerging skill demands, as they are collected daily from available jobs posted online in quasi real-time. Furthermore, OJPs provide very granular information on skill demands, allowing for a more detailed analysis of the specific technologies and skills in high demand across the cyber security landscape. Despite the advantages, OJPs have limitations, as they may not provide comprehensive coverage of some occupations and sectors where vacancies are not typically advertised through online platforms (see Cammeraat and Squicciarini (2021[4]) and OECD (2021[5])).

This chapter investigates the demand for cyber security professionals in Chile, Colombia, and Mexico in 2021 and 2022 using data collected by Lightcast[1] from nearly 14 million OJPs over a two-year period. The remainder of this chapter is organised in two sections. The first section overviews the recent demand for cyber security professionals in the three Latin American countries. The second section explores in detail the skills required by employers seeking cyber security workers, according to the texts available in the OJPs. Box 2.1 includes some methodological notes useful for interpreting the results.

Box 2.1. Methodological note: Interpreting the results from online job postings

The wealth of information contained in job postings can offer a very detailed overview of the demand of enterprises for cyber security profiles. This box summarises the main methodological approaches used to leverage these data and improve the readability of the results and insights shown below. Annex 2.A and the footnotes of each figure provide additional details.

Using OJPs to identify the recent evolution of demand

- **Cyber security OJPs:** Data from Lightcast for Latin American countries do not explicitly include a "cyber security occupation title". Instead, job postings are mapped to occupations using the International Standard Classification of Occupations (ISCO-08). This occupational taxonomy is, however, too aggregated to identify cyber security professionals specifically. To identify cyber security job postings in 2021 and 2022, this report instead uses a text mining approach applied directly to the underlying detailed job titles extracted from each online job posting. Annex 2.A provides more details on the keywords used to identify a job posting as cyber security-related.
- **Cyber security roles:** Using the job titles available in OJPs, this chapter disaggregates data into roles and tracks the demand for each. Four specific roles were chosen (Analysts, Architects and engineers, Auditors and advisors, and Managers) by extracting the most frequently used keywords from cyber security job advertisements. Annex Table 2.A.2 contains the comprehensive list of keywords associated with each role.
- **Groups of digital, engineering and math-related occupations:** The analysis provides insights on 25 occupations used as benchmarks to compare the trends in their demand with the demand for cyber security professionals. The 25 occupations were classified into 5 occupational groups: 1) Computer and data analysts/administrators; 2) Software developers and programmers; 3) ICT technicians; 4) Math-related professions; and 5) Engineers and technicians.

Using information from OJPs to infer skill demands in the cyber security profession

- **Skill bundles**: Using Natural Language Processing (NLP) methods, the analysis in this chapter identifies the most relevant technical and professional/transversal skills in employer demands cyber security positions collected through OJPs in Chile, Colombia and Mexico (more details can be found in Annex 2.A). Technical skills refer to "*specialised skills, knowledge or know-how needed to perform specific duties or tasks*" (UNESCO - UNEVOC, 2023[6]), while professional/transversal skills are those "*not specifically related to a particular job, task, academic discipline or area of knowledge and that can be used in a wide variety of situations and work settings*".
- **Skills relevance**: As detailed in Annex 2.A, the "skill relevance" index should be interpreted as a measure of the relevance of a given skill for the cyber security profession. The closer the value assigned to a certain skill is to one, the higher the relevance of the skill for the occupation.

  It is also important to note that some of the keywords collected do not represent skills *strictu sensu.* Some of them, for instance, are technologies or tools (i.e. Python or Microsoft Azure), while others identify knowledge areas (i.e. Network or Information Security). For the sake of simplicity, this study pools all keywords together under the term "skills" and only differentiates between them if necessary.

The demand for cyber security professionals in recent years

Most cyber security professionals are in charge of securing data, systems, infrastructure and other cyber resources from failures, hazards and cyber threats that affect an organisation's mission and operation (World Economic Forum, 2022[7]). This section focuses on tracking the demand for these professionals in Chile, Colombia and Mexico over 2021 and 2022, using online job postings (OJPs). As mentioned, this report uses text mining techniques, by investigating the text contained in job titles, to determine which OJPs are looking for cyber security personnel (more details can be found in Annex 2.A).

How has the demand across countries evolved?

In recent years, Latin America has experienced a notable surge in the demand for cyber security professionals, as evidenced by the rise in online job postings in the countries analysed in this report (see Table 2.1). This trend highlights the growing recognition of the crucial role cyber security plays in the region's digital landscape, something that is echoed across in other regions as well. For instance, (OECD, 2023[8]) shows that especially after 2020, the demand for cyber security professionals in five anglophone countries increased significantly. As technology advances and cyberspace becomes increasingly intertwined with everyday life, Latin American countries are grappling with the urgent need to address cyber threats.

The data in Table 2.1 reveal a common trend of growing demand for cyber security professionals across all three Latin American countries examined in this report. In particular, the data reveal that the growth for cyber security professionals in between 2021 and 2022 was faster than for all occupations combined in both Chile and Mexico.

Table 2.1. Growth rates of cyber security professionals in LATAM countries

Country	Growth rate for cyber security professionals	Growth rate for other professions
Chile	28.7%	2.9%
Colombia	20.9%	19.0%
Mexico	64.6%	27.3%

Note: Growth rates have been calculated by comparing the total number of OJPs between January and December 2022 to those between January and December of 2021.
Source: OECD calculations based on Lightcast data.

Zooming in at the country level, results in Table 2.1 show that the demand for cyber security professionals in Chile grew by 28.7%, a figure that is substantially higher than the growth rate for other professions, which stands at 2.9%. Behind this tenfold larger increase in the demand for cyber security professionals in Chile there is the increasing emphasis that the country has put in developing its cyber ecosystem in recent years. In 2017, the government instituted the National Cyber Security Policy 2017-22, which identified concrete goals with the purpose of promoting and ensuring a free, open, safe and resilient cyberspace (UNODC, 2017[9]), see Box 2.2. Furthermore, Chile suffered from a large cyber security attack in 2018, when hackers stole USD 10 million from the Banco de Chile (Kirk, 2018[10]). This again renewed the attention on cyber security. Focus continued into 2020, as the Computer and Security Incident Response Centre (CSIRT-CL) reported over 2.3 billion cyberattack attempts in that year (CSIRT, 2021[11]). Lastly, 2022 was the year that the government issued a modernised cyber security law, which updated the previous regulatory and institutional framework that was established from 1993 (See Box 2.2). (Council of Europe, 2022[12]).

The steep growth in cyber security jobs in Chile is contrasted with relatively low growth in online job postings (OJPs) for all professions. While the Chilean economy experienced a strong recovery in 2021 after the peak of the COVID-19 crisis as GDP grew by 11.9% (OECD, 2022[13]), GDP growth slowed down in 2022 to 2.4% (Banco Mundial, 2023[14]). Production in Chile decreased during the first quarter of 2022 and has remained lower compared to the previous year. Additionally, the government has withdrawn support measures that were initially implemented to mitigate the economic consequences of the pandemic. Consequently, these factors have resulted in slowed consumption, further impacting the overall demand for professionals across all sectors. (OECD, 2022[13]).

Box 2.2. Chile's national cyber security policy and legal framework

Cyber security policy

In 2016 the Chilean Government created a national cyber security policy, which would span from 2017 until 2022. The intent of this policy was to help protect people's security and manage threats in cyberspace, as well as to protect the country's security and to promote co-operation and co-ordination between institutions. The policy objectives that were determined to achieve these goals are" (UNODC, 2017[9]):

1. "The country will have in place a robust and resilient information infrastructure, prepared to face and recover from cybersecurity incidents, under a risk management approach"
2. "The State will protect people's rights in cyberspace."
3. "Chile will develop a cybersecurity culture based on education, good practices and accountability in the management of digital technologies."
4. "The country will carry out co-operation actions with other stakeholders in the field of cybersecurity and will actively participate in international forums and discussions."
5. "The country will promote the development of a cybersecurity industry serving its strategic objectives."

To be able to better achieve the goals in the national cyber security policy, Chile created a Computer and Security Incident Response Centre known as CSIRT-CL in March of 2018. This CSIRT is responsible for providing information and assistance to the government cyberspace; administering a system of co-operation on cyber security; promoting good practices in cyber security within the government administration; promoting the protection of critical information infrastructures and key resources of the country; promoting the strengthening of the legal framework as it relates to computer and cybercrime; and promoting awareness on cyber security. (Council of Europe, 2022[12])

Legal framework

The Chilean Government instituted a new cyber security law in 2022 to modernise the existing legal framework, which stemmed from 1993, and bring it into accordance with the Budapest Convention (Council of Europe, 2001[15]). The new law criminalises offences such as unlawful access and interception of information and computer systems, attacks on the integrity of computer data or computer systems, abuse of devices, computer forgery and computer fraud. It also exempts criminal liability for 'ethical hacking' practices". (Council of Europe, 2022[12])

Results in Table 2.1 show that in Colombia the growth rate for cyber security professionals was significant and above 20%. However, the growth in demand for these professionals remains aligned with the average growth experienced in the online labour market for non-cyber security occupations.

The high growth rate for cyber security professions in Colombia can be linked to the country's context of improvements to the cyber security regulatory framework for more than a decade, see Box 2.3. The Colombian Government adopted a national cyber security policy for the first time in 2011, followed by a second policy in 2016 (IADB & OAS, 2020[16]). In 2020 they proposed the new "national trust and digital security policy (2020-22)" (OAS & CISCO, 2023[17]). Laws that govern cybercrime have been in place since 2009, while laws surrounding data protection and privacy were instituted in 2012 (IADB & OAS, 2020[16]).

The overall high growth of OJPs in Colombia between 2021 and 2022 is accompanied by a GDP growth of 8.1% in 2022 and a strong employment recovery in the first half of 2022 (OECD, 2022[13]). Furthermore, the Colombian central bank reported that the labour market in 2022 was tight, meaning that there was a relatively large number of vacancies compared to the number of unemployed workers (La República, 2023[18]).

Box 2.3. Colombia's cyber security framework

Cyber security policies

Whereas the first version of Colombia's cyber security and cyber defence policy from 2011 focused on counteracting the increase in cyber threats in order to protect the country; and to fight against cybercrime, the second version which was instituted in 2016 increased its focus on risk management in the digital environment. This second policy "sets a roadmap with the purpose of identifying, managing, processing, and mitigating digital security risks in the socio-economic environment." (MinTIC, 2016[19])

The third policy, the national trust and digital security policy instituted in 2020, instead focuses on establishing digital trust in Colombian society, with the following specific goals (MinTIC, 2020[20]):

1. "Strengthen the digital security capabilities of citizens, the public sector and the private sector to increase the digital confidence in the country".
2. "Update the digital security governance framework to increase its degree of development and improve the progress in digital security in the country."
3. "Analyse the adoption of digital security models, standards, and frameworks, with an emphasis on new technologies to prepare the country for the challenges of the fourth industrial revolution."

Legal framework

In 2009, the Colombian Government enacted a few laws on cybercrimes, which protected information, data and ICT systems, as well as defined the concepts necessary for this digital environment. In 2011 the laws were updated with amongst others a regime for the protection of the rights of users of communication services and an obligation for internet providers to use technical and logistical resources to guarantee the security of the network and the integrity of the service, to avoid the interception, interruption and interference. (MinTIC, 2016[19])

In Mexico, the growth of cyber security OJPs was 2.4 times that of the growth rate for all OJPs. The total number of cyber security OJPs went from 3 328 in 2021 to 5 314 in 2022, an increase of nearly 65%, whereas the overall number of OJPS grew by 27% (Table 2.1).

The pronounced increase in cyber security OJPs is driven by the continually increasing need for cyber security professionals, as Mexico is one of the countries in Latin America that is most often targeted in cyber attacks, which can have far-reaching economic consequences. For instance, just like in Chile, Mexican banks were the target of cyber attacks in 2018, and 5 banks experienced losses as high as USD 20 million (Kirk, 2018[21]). Furthermore, Mexico is still one of the top victims of attacks in Latin America, as "85 billion cyberattacks were attempted in Mexico in the first half of 2022, according to the Mexican Cyber security Association (AMECI), an increase of 40% over the same period in 2021." (INAI, 2022[22]). Moreover, FortiGuard Labs, a cyber intelligence laboratory, reported that Mexico received more than half of the attacks reported in Latin America during 2022 (187 billion), followed by Brazil (103 billion) and Colombia (20 billion) (FortiGuard Labs, 2023[23]).

Mexico is aware of the need for more cyber security, as evidenced by the national cyber security strategy which the government created in 2017 (Government of Mexico, 2017[24]), see Box 2.4. And while the country does not currently have a dedicated law on cybercrime (IADB & OAS, 2020[16]), a new federal law on cyber security has been proposed to the chamber of deputies in April of 2023 (Cámara de Diputados, 2023[25]), see Box 2.4.

Although the growth in the number of cyber security OJPs is much stronger than that for the overall number of OJPs, which is also highly significant at 27%. Mexico's labour market improved in 2022, as a gradual recovery in tourism and in internal consumption led to slightly higher employment in the summer of 2022, than at the end of 2019, before the COVID-19 pandemic (OECD, 2022[26]). This helped propel the number of OJPs posted in Mexico.

Box 2.4. Mexico's national cyber security strategy and legal framework

National cyber security strategy

Mexico's cyber security strategy from 2017 has the "main objective of identifying and establishing the cyber security actions applicable to social, economic, and political areas, to enable citizens and private and public organisations to use ICTs responsibly for the sustainable development of the Mexican state". (Government of Mexico, 2017[24]). There is a strong focus on improving people's ability to operate in a safe digital environment. In order to achieve these goals, the following strategic objectives were formulated (Government of Mexico, 2017[24]):

1. "Create the conditions for the population to carry out activities responsibly, freely, and in a safe manner in cyberspace. Improve the quality of life through digital development [...]"
2. "Strengthen cyber security to protect the economy of different sectors of the country and promote technological development and innovation. Boost the national cybersecurity industry, in order to contribute to economic development [...]."
3. "Protect information and computer systems of public institutions to ensure their optimal functioning and the continuity in the provision of services. "
4. "Improve capacities for the prevention and investigation of criminal behaviour in cyberspace that affect people and their assets, with the aim of maintaining order and public peace."
5. "Develop capacities to prevent risks and threats in cyberspace that may alter national sovereignty, integrity, independence, and impact development and national interests."

Legal framework

The provisions in regard to cybercrime in the currently existing laws are limited, leading to difficulties in combatting these crimes (IADB & OAS, 2020[16]). Part of the national cyber security strategy was to aim at adapting the national legal framework. As a result, the newly proposed cyber security law stemming from April 2023 proposes changes to the framework. The law -if adopted- will define cybercrimes and "establish the attributions, powers and responsibilities between authorities". It also proposes a new national cyber security agency and makes registering with this agency mandatory for any digital platform operating in the country (Paez Jiminez, 2023[27]).

While the demand for cyber security professionals has been on the rise across the countries examined, the total number of OJPs for cyber security jobs remains a relatively small share of the total number of OJPs in each Latin American country analysed in this report. On average in 2021 and 2022, 0.08% of all OJPs in Chile were looking for cyber security professionals, compared to 0.13% in Colombia and 0.11% in Mexico. One reason why the share of cyber security jobs might seem smaller in Chile than in the other two countries analysed, could be attributable to the fact that Chile's informal sector is relatively smaller (30% of labour is informal in Chile compared to 55%-60% in Colombia and Mexico) and that many more jobs across other sectors are captured by OJPs in this country. It is worth noticing that most of the cyber security jobs are indeed in the formal sector, and OJPs are likely to be a good representation of the demand for these types of professionals. However, other jobs that are part of the informal sector might not be captured by OJPs. This means that the total share of cyber security vacancies, if informal jobs are taken into account, might be lower for Colombia and Mexico as well.

As Latin America's digital landscape evolves and the region becomes more integrated into the global digital economy, the demand for cyber security professionals is likely to increase. Countries have stated that cyber resilience is a priority to also be able to benefit from the digital transition.

Zoom in: What are the job roles in high demand within the cyber security landscape?

Online job postings can provide a detailed overview of the demand for specific cyber security professionals/roles within the cyber security landscape. This section leverages the job titles used in advertisements to categorise them into different roles, following the approach applied in recent OECD work (OECD, 2023[8]).[2] The roles analysed are cyber security analysts, architects and engineers, auditors and advisors, and managers. The distribution of the demand across different cyber security roles in Chile, Colombia and Mexico follows a pattern similar to the one observed in the Anglophone countries analysed in OECD (OECD, 2023[8]) (i.e. Australia, Canada, New Zealand, the United Kingdom and the United States), with analysts and architects/engineers representing 60%-65% of the total OJPs for cyber security professionals.

According to the NICE Cybersecurity Framework of the U.S. National Institute of Standards and Technology (NIST), cyber security architects are responsible for securely provisioning IT systems. This involves designing and modelling security solutions that address business security needs adequately (NICCS, 2023[28]). Engineers, on the other hand, work closely with architects and focus on the processes required for implementing security solutions and integrating them with other IT products (Joint Task Force Transformation Initiative, 2018[29]). Cyber security architects/engineers develop comprehensive security solutions, design infrastructure configurations, and integrate various security technologies. Their expertise is vital in ensuring that organisations' digital infrastructure is resilient against cyber attacks and that security measures are integrated into the core design of systems and applications. Cyber security analysts are responsible for performing highly specialised reviews and evaluations of cyber security information to gain insights that support the planning, operations, and maintenance of IT systems security (NICCS, 2023[30]). They are responsible for analysing and interpreting security data, identifying vulnerabilities, and implementing appropriate measures to mitigate digital security risk. The NICE Cybersecurity Framework defines a special category for this role, including specialty areas such as exploitation/vulnerability, language, and threat analysis. With the evolving nature of cyber threats, organisations require skilled analysts who possess a deep understanding of cyber-attack techniques, threat intelligence, and incident response protocols. The high demand for cyber security analysts suggests that firms and governments are actively seeking to enhance their threat detection and response capabilities to safeguard their digital assets and sensitive information.

The demand for cyber security architects/engineers is particularly strong in Chile where they represent 40% of the total number of OJPs advertised during 2021 and 2022. In Mexico, 34% of the cyber security OJPs seek architects/engineers, being also the role with the highest share of cyber-related OJPs, while in

Colombia, this role accounts for 30% of cyber security OJPs. The high demand for cyber security architects/engineers across Chile, Colombia, and Mexico underscores the critical need for skilled professionals in the field, reflecting the increasing recognition among organisations of the importance of robust cyber security measures and the rising prevalence of cyber threats.

Mexico is the only country among those analysed in this report that experienced positive growth across all cyber security roles between 2021 and 2022. This result confirms the country' thriving cyber security labour market. However, the observed positive growth in the number of new cyber security job postings may also reflect the increasing risk that Mexican organisations face in the cyber space. As pointed out in the previous subsection, reports indicate that Mexico is receiving the highest number of cyber attacks in the region.

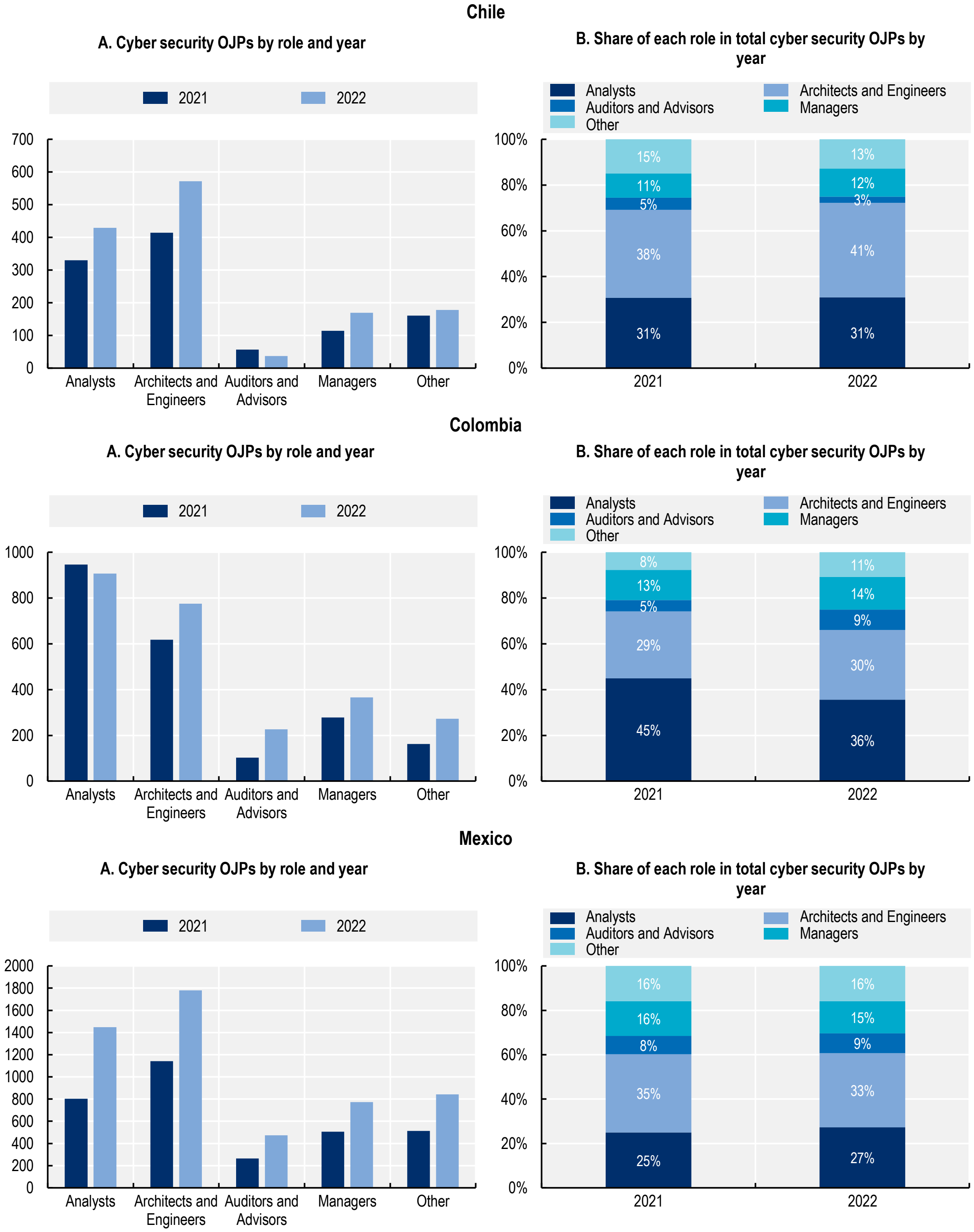
In Mexico, the role with the strongest growth, measured by the increase in the number of new OJPs, is analysts, for which demand has expanded by 80% between 2021 and 2022. On average, analysts represent 26% of the cyber security OJPs advertised in Mexico. Managers experienced a growth of 53% in the same period, representing an additional 15% of the cyber security OJPs (Figure 2.1, Panel B). According to the NICE Cybersecurity Framework, managers fall into the category of "oversee and govern," which includes all positions in charge of providing leadership, management, and direction to cyber security teams in an organisation. Specifically, this classification defines cyber security managers as these professionals overseeing the cyber security programme of an information system or network and managing information security implications within different areas of responsibility (NICCS, 2023[30]).

In Chile, managers and architects/engineers stand out as the roles with the strongest growth between 2021 and 2022, 48% and 38% respectively. Analyst, the second most in-demand role, also experienced a significant growth of 30%. In contrast, auditors and advisors decreased nearly 35%, which implied that less than 3% of cyber security OJPs advertised in Chile during 2022 were seeking for this type of professionals. This role includes professionals who provide external or internal advice about the efficiency and compliance of security solutions.

In Colombia, the analysis of the demand for cyber security roles shows different results. While analysts, the most in-demand role, experienced a decrease of 4% between 2021 and 2022, architects/engineers and managers presented positive growth of 26% and 32%, respectively. Despite being the least demanded role, the demand for cyber security auditors and advisors increased by 120%. A closer look at the job titles used in cyber security OJPs in Colombia shows that the most in-demand positions for this role are information security consultants and cyber security auditors.

The significant increase in demand for cyber security auditors and advisors in Colombia indicates a growing recognition among organisations of the importance of assessing the efficiency and compliance of their security solutions.[3] This trend reflects an evolving understanding of the critical role that auditing and advisory services play in ensuring the effectiveness of cyber security measures. In particular, organisations increasingly realise that cyber security is not solely about implementing preventive measures but also about regularly evaluating and verifying the efficacy of those measures. Cyber security auditors and advisors provide valuable expertise in assessing the overall security posture of an organisation, identifying vulnerabilities, and recommending improvements. In that, they play a crucial role in ensuring that security solutions are not only implemented but also continuously evaluated and optimised to align with changing threat landscapes and industry best practices.

Figure 2.1. Cyber security roles: Recent evolution and shares



Source: OECD calculations based on Lightcast data.

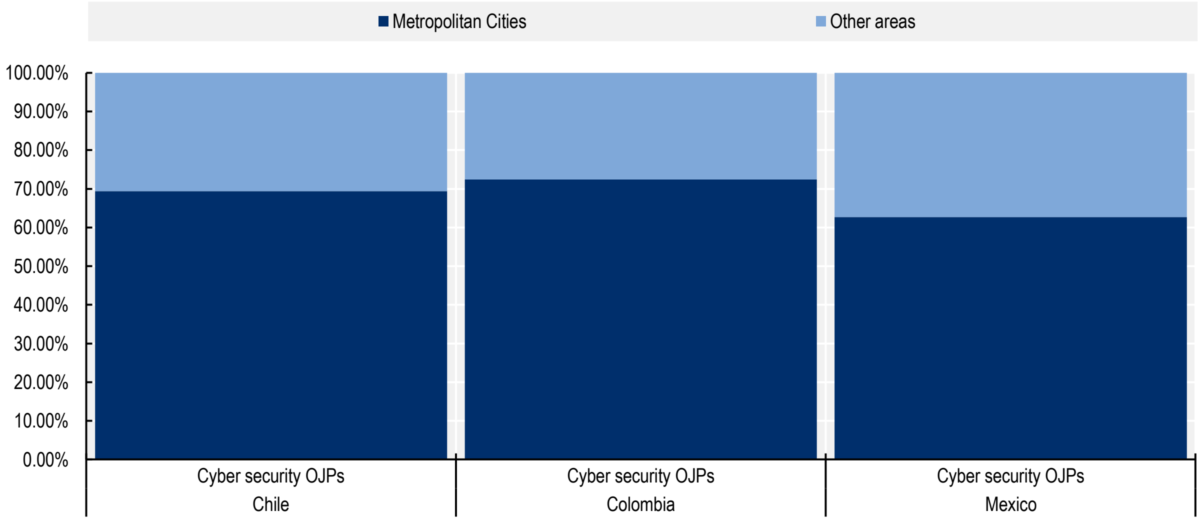
Where is the demand for cyber security professionals located?

Chile, Colombia and Mexico all have stark economic and demographic divides between urban and rural areas. All three countries have highly geographically concentrated populations, ranking 4th, 5th and 6th of all OECD countries in terms of the geographic concentration index of the population in 2019.[4] This goes hand in hand with high rates of urbanisation, especially in Colombia, where 57% of the population lives in a metropolitan region compared to an OECD average of 41.4%. The shares of the populations living in a metropolitan region are, instead, much lower for Chile and Mexico, at 30 and 34.7%, respectively, although certain cities in Mexico, like Mexico City, have millions of inhabitants. So, while Chile and Mexico are highly demographically concentrated, most of their urban areas are smaller than those in Colombia. (OECD, 2022[31])

It is, therefore, interesting to examine where the job opportunities for cyber security professionals are located by comparing the share of cyber security OJPs in metropolitan cities[5] to the shares in other areas. The distribution for all OJPs is instead described in Box 2.5. For the analysis, metropolitan cities are classified as cities with 250 000 inhabitants or more. According to the latest censuses, there are 71 metropolitan cities in Mexico, 28 in Colombia and 11 in Chile (INEGI, 2020[32]; DANE, 2018[33]; INE, 2017[34]).

In all three countries, the share of cyber security OJPs posted in metropolitan cities is substantial (Figure 2.2). More than 60% of cyber security OJPs[6] are concentrated in these larger urban areas. For instance, in Mexico, 62.7% of cyber security OJPs target personnel in metropolitan cities, which exceeds the proportion of the Mexican population residing in metropolitan areas (34.7%) (OECD, 2022[31]).

Figure 2.2. Share of (cyber security) OJPs that are posted in metropolitan cities



Note: The share of cyber security OJPs without information on the city is 77% in Chile, 23.2% in Colombia and 38.5% in Mexico.
Source: OECD calculations based on Lightcast data.

Box 2.5. OJPs in metropolitan cities

Figure 2.2 shows the distribution of cyber security OJPs that are posted in metropolitan cities. The purpose is to analyse the geographic concentration of cyber job postings. The figure does not show the same distribution for non-cyber security OJPs, as there may be issues with the representativeness of the data for all labour demand.

As explained in Box 1.3 informality is unlikely to introduce a bias on the number of cyber job postings that are observed. Furthermore, cyber security roles are more likely to be advertised online than other low-skill and medium-skill positions, as these roles are often high-skill positions. The sample for cyber security is therefore most likely representative for the actual labour demand.

However, the same reasoning does not apply to OJPs for other occupations. The shares of all OJPs that are posted in metropolitan cities are: 40.1% in Chile, 72.7% in Colombia, and 58.9% in Mexico. In this case, the large informal sectors and the underrepresentation of low- and medium-skill jobs can result in a lower number of OJPS in rural areas compared to the actual labour demand in these regions. Crucially, these problems are likely to be more pronounced in rural areas than in urban areas (European Parliament, 2021[35]) which means that the shares on the geographic distribution of OJPs for all occupations are not as informative as for the cyber security roles.

Source: OECD calculations based on Lightcast data.

One reason why more cyber-related job opportunities are found in metropolitan cities could be that certain industries, such as finance, technology, and professional services, tend to have a higher presence in metropolitan areas due to the availability of skilled labour, infrastructure, and market demand. Cities, for instance, have higher levels of tertiary attainment and more institutes for higher education (OECD, 2022[36]). Labour markets also provide strong incentives for tertiary-educated workers to move to urban areas, as wages are often higher there (OECD, 2022[36]). The previously mentioned industries benefit from highly educated personnel, making cities attractive spaces to locate. Advanced types of industries are also more likely to hire cyber security professionals. At the same time, however, high-skilled jobs are more likely to be posted online (Cammeraat and Squicciarini, 2021[4]), which can lead to overrepresentation of the share of OJPs that are posted in metropolitan cities, while informality can lead to underrepresentation of low-skilled jobs in non-urban areas.

The results for Chile demonstrate the largest disparity between the share of people residing in metropolitan cities and the share of cyber security OJPs. Just 30% of the Chilean population lives in a metropolitan area (OECD, 2022[31]), while nearly 70% of cyber security OJPs can be found there. However, previous research also showed that "the majority of the OJPs in the cyber security job market are for jobs located in main urban areas where major enterprises and government headquarters are found" (OECD, 2023[8]). The same holds for Chile, where the majority of job opportunities in cyber security are posted in Santiago, for example within companies such as (IT) consultancy firms, accounting firms, and research companies.

In Mexico, a noteworthy cyber-related industry is that of production of (consumer) electronics. As of 2022, there are 487 different manufacturers of electronics in Mexico, mostly in the states Baja California and in Jalisco, which are home to 7 different metropolitan cities: Tijuana, Mexicali, Ensenada, Guadalajara, Zapopan, Tlaquepaque, and Tonalá (Government of Mexico, 2022[37]). The country is known for its role in global supply chains, particularly within the electronics sector, thanks to its strategic location, abundant labour supply, and numerous trade agreements. The electronics manufacturing industry in Mexico includes production of telecommunication equipment, electronic appliances, computers and computer peripherals, and other consumer electronics, and the production of electronics in Mexico has experienced a rapid growth following the outbreak of the pandemic in 2020. Exports of electrical machinery and equipment from Mexico reached USD 87 billion in 2021, positioning the country as the world's 9th largest exporter in this field (United Nations Statistics Division, 2023[38]). 28%[7] of Mexican cyber security OJPs in 2021 and 2022 are posted in the manufacturing industry, and most of these advertisements are within the electronics industry, within the earlier mentioned metropolitan cities.

In Colombia, although a larger percentage of the population (57%) resides in metropolitan areas compared to Mexico and Chile (OECD, 2022[31]), an even larger share of cyber security OJPs are posted in metropolitan cities (around 73%). Opportunities for cyber security professionals are found across a wide variety of industries in cities, signalling how the awareness of the need for cyber security has permeated companies in all different branches. Some notable industries for cyber security professionals in Colombia are the information industry, as well as professional, scientific, and technical services, with most of the OJPs being located in Bogotá and Medellín. Companies that operate within the information sector are often large telecom providers, as well as technology firms. These types of companies can face significant cyber threats and will need to make sure they have secure networks and are in charge of safekeeping a lot of data (like cloud storage). Companies that work on research and development and are part of the professional, scientific, and technical services benefit from having a highly educated workforce, which is why they are often located in the metropolitan cities, close to institutes for tertiary education. Companies that work on development also have large incentives to safeguard their data, leading to an increased need for cyber security.

What is the demand for digital, engineering and math-related occupations?

Global trends such the digital transition and the creation of new technologies do not only propel the demand for cyber security professionals, but also affect the demand of related (digital) occupations. Employers increasingly adopt cloud computing, artificial intelligence and make more use of data. While these developments lead to opportunities for economic growth on the one hand, on the other hand they also lead to more potential cyber security threats, which necessitates a skilled cyber security workforce (IADB & OAS, 2020[16]).

Demand for digital, engineering and math-related occupations has been growing for a long time, while the need for cyber security is also becoming increasingly more pressing as digital technologies are adopted in LATAM. For instance, in Colombia technology and digitisation have already led to innovation in commercial, productive, and scientific research, with Colombia's tech sector growing significantly over the last few years. The aspirations are that this will turn the country into "the Silicon Valley of Latin America". Software and IT services' exports amounted to USD 218.8 million in 2021, a 33% increase from 2020, which shows that this focus on science, innovation and technology is leading to concrete benefits for the Colombian economy (Moncayo and Guzmán, 2022[39]). However, technological systems are often still vulnerable to cyber security threats, espionage and breaches of information (Moncayo and Guzmán, 2022[39]).

This section aims to explore the relationship between the demand for cyber security professionals and other digital, engineering and math-related occupations, contributing to a nuanced understanding of the evolving digital landscape and how data usage and digitalisation has permeated the labour market. By examining the demand for cyber security professionals alongside other related roles, this analysis seeks to discern patterns, identify potential skill gaps, and derive comprehensive insights into the broader dynamics shaping the contemporary job market.[8]

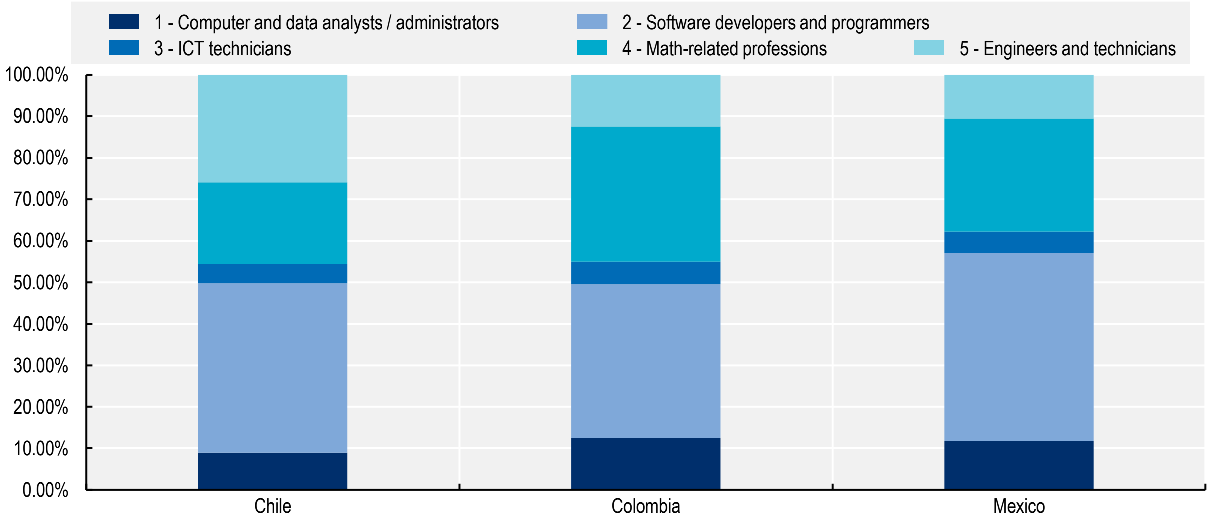
This section analyses 25 occupations that are classified into five occupational groups to assess the relationship between their demand (approximated by the growth in OJPs) and that for cyber security professionals. The choice of these occupational groups is based on the methodology used in two recent OECD reports (OECD, 2022[40]; 2023[8]) but it has been refined for this report into five occupational groups:

1) Computer and data analysts / administrators; 2) Software developers and programmers; 3) ICT technicians 4) Math-related professions; and 5) Engineers and technicians.[9]

The average share of OJPs for digital, engineering and math-related jobs over the period 2021 – 2022 is below 10% in all three countries, at 6.4% in Chile, 7.3% in Colombia and 5.6% in Mexico. However, it should be noted that all of these jobs are more likely to be advertised online than jobs in other occupations as they are high-skill occupations (Cammeraat and Squicciarini, 2021[4]), which means that these shares might be an overrepresentation of the share over the total labour market demand.

In all three countries, the group of digital, engineering and math-related occupations with the highest demand, as indicated by the number of OJPs, is software developers and programmers (comprising the ISCO occupations: web and multimedia developers; applications programmers; software developers; and software and applications developers and analysts not elsewhere classified), see (Figure 2.3). In Chile, software developer and programmers represent 40.8% of the OJPs for digital, engineering and math-related jobs, compared to 37% in Colombia and 45.4% in Mexico respectively.

Figure 2.3. Distribution of the digital, engineering and math-related jobs in 2021 and 2022



Source: OECD calculations based on Lightcast data.

Other indicators also show that software development is becoming an increasingly important industry in Latin America. For instance, in Mexico the number of people trained to be software developers nears 700 000, with Mexican software developers ranking highly in terms of their skills on several different evaluations (Tecla, 2023[41]). Due to its location, companies from the United States also often outsource/nearshore their software development to Mexico, which is another driver for the demand for these professionals (Taplin, 2022[42]).[10]

Within the broader group of software developers and programmers, software developers by themselves (ISCO 2 512) represent the most highly demanded occupation, as 26%, 23%, and 29% of all digital, engineering and math-related OJPs are for software developer jobs in Chile, Colombia and Mexico respectively. Other sources also report a high need for software developers, for instance the Ministry of ICT in Colombia estimates that in 2022 there was a shortage of 80 000 software developers in Colombia, which is expected to increase to 112 000 in 2025 (González, 2022[43]).

Notably, the tasks that software developers are expected to perform are often very closely aligned with those of many cyber security employees. For instance, the responsibilities of software developers involve designing, developing, testing, and maintaining software solutions (ISCO-08), tasks that are often shared with cyber security professionals, such as cyber security architects/engineers. These cyber security professionals develop comprehensive security solutions, design infrastructure configurations, and integrate various security technologies. The relatively large share of software developer OJPs suggests that more and more, digital roles are permeating Latin American labour markets and that the demand for those professionals is poised to lead to an increase in digitalisation and, as a consequence, of cyber threats and the need to develop a cyber-skilled workforce.

In Chile a significant volume of digital, engineering and math-related OJPs is allocated to engineers and technicians, accounting for 25.9% of these OJPs compared to 12.5% in Colombia and 10.5% in Mexico. The most highly demanded type of engineers in Chile are civil engineers, with a total number of OJPs of 30 427. Civil engineers nowadays “deal with the management of urban and rural systems, dealing with aspects such as disaster prevention, traffic control, water resource management, garbage treatment and all those activities necessary for well-being of the society.” (Universidad De Chile, 2023[44]).

These new responsibilities for civil engineers require an increased reliance on data and on a good cyber infrastructure. Heightened importance of data brings with it a rise in cyber security threats, such as data breaches, data manipulation vulnerabilities, and being the target of ransomware. Cybercriminals can seek to gain access to sensitive information, which can lead to for instance the theft of personal data, financial information, or trade secrets, or alter data to deceive companies and governments or encrypt data and demand ransom in exchange for decryption. To be able to counter these threats, a skilled cyber security work force is necessary, as well as improved cyber skills for other professionals more generally.

Overall, math-related professions have a larger presence in terms of volumes of new online job postings in Colombia (32.5% of digital, engineering and math-related OJPs) and Mexico (27.3%), compared to Chile (19.6%) (Figure 2.3).[11] Financial and investment advisers are the most highly sought-after role within the group for both Colombia and Mexico. For instance, in total there are around 58 900 OJPs specifically looking to hire people for this role in Colombia in between 2021 and 2022. The financial sector is one that bears important ties with cyber security. Financial and investment advisers “develop financial plans for individuals and organisations and invest and manage funds on their behalf” (ISCO-08). This is a role in which mathematical abilities, analytical thinking and a grasp of information technology are highly valued (Indeed, 2023[45]). Furthermore, (big) data is increasingly more important in finance, which means that finance companies are also more likely to need to hire cyber security specialists to make sure that data is protected.

To put it in other words, the financial sector is becoming increasingly digitalised, fuelling the need for robust cyber security measures. Cyber security professionals have thus become invaluable assets within this sphere, given the industry’s significant dependency on data and networked systems. Financial institutions manage vast amounts of sensitive information, including customer financial data and confidential business intelligence. Breaches can result in considerable financial losses, damaged reputations, and regulatory penalties. Additionally, the financial sector is an attractive target for cyber criminals due to the potential profitability of such data. Therefore, cyber security professionals are crucial for implementing protective measures, such as encryption, firewall configuration, and intrusion detection systems, to safeguard this information. They also play a pivotal role in mitigating attacks, responding to breaches, and ensuring business continuity. As technology continues to evolve, threats become more sophisticated, increasing the demand for these professionals. Consequently, the relationship between the financial sector and cyber security is symbiotic, underpinned by the need to protect valuable data in an increasingly interconnected and risky digital landscape.

The professional profile required in cyber security online job postings

The skills bundle of cyber security professionals

The widespread adoption of digital technologies, coupled with the emergence of new cyber threats, is constantly reshaping the skill requirements for cyber security professionals. This dynamic and highly technical environment presents challenges for both the demand and supply sides of the labour market. On the supply side, workers often struggle to develop the essential skills needed to enter and progress in the cyber security job market. While, on the demand side, organisations also face difficulties in accurately identifying the necessary skill requirements to effectively fill vacancies and retain top talent in the field (OAS & CISCO, 2023[17]).

To foster the development of a skilled cyber security workforce in the region, it is crucial to establish a common framework that reduces mismatches and foster alignment between the demand and supply sides. The efforts made by Chile, Colombia, and Mexico to develop cyber security policies that recognise the importance of workforce capacity building are commendable. However, the effectiveness of these policies will also depend, to some extent, on the data available to characterise skills demand and supply in the sector. Traditional labour market data lack the necessary detail and timeliness to accurately capture them. Analysing online job postings can bridge this gap effectively, providing policy makers with valuable insights into the specific skills in demand and emerging trends. This approach enables policy makers to tailor their capacity-building efforts, respond to evolving labour market needs, and foster a skilled workforce that can thrive in the dynamic cyber security landscape.

This section examines the specific skill requirements mentioned by employers in cyber security online job postings. The objective is to shed light, from the demand side, on the skill set that typically characterises the demand of employers seeking cyber security professionals. In particular, the analysis presented in Figure 2.4 employs Natural Language Processing (NLP) techniques (see Box 2.6) to identify the most relevant technical and professional skills required by employers in each country analysed. As outlined in Box 2.1, technical skills refer to specialised knowledge or expertise required to perform specific tasks within the profession, while professional/transversal skills encompass broader skills not limited to a particular job or discipline but applicable in various situations or work environments.

The data presented in Figure 2.4 indicate that there are two skills that are commonly required across all three countries: familiarity with principles related to ISO/IEC 27001 standard and knowledge of Security Information and Event Management (SIEM).

The ISO/IEC 27001 refers to a collection of requirements, guidelines, and best practices developed by the International Organisation for Standardization (ISO) and the International Electrotechnical Commission (IEC) that formally specifies an Information Security Management System (Microsoft, 2023[46]). It provides a structured approach to identifying threats, implementing security controls, and ensuring the confidentiality, integrity, and availability of information assets. This standard facilitates communication and collaboration among professionals working in the field of cyber security. In addition, many regulatory frameworks and industry-specific standards reference ISO/IEC 27001 as a benchmark for information security. Familiarity with the ISO/IEC 27001 principles is, therefore, crucial for cyber security professionals as this serves as a recognised standard for managing and protecting sensitive information.

On the other hand, SIEM (Security Information and Event Management) is a technology solution that combines information security information management (SIM) and security event management (SEM) tools to provide real-time monitoring, threat detection, and incident response capabilities. SIM helps collecting and aggregating logs and event data from various sources within an organisation's IT infrastructure. This centralised log management enables efficient monitoring and analysis of security events, making it easier to identify potential threats and security incidents. SEM analyses the collected data in real-time, using correlation rules, statistical analysis, and machine learning algorithms to detect patterns indicative of security breaches, attacks, or policy violations. In recent years, the incorporation of machine learning and AI in SIEM systems has contributed to a more automated and intelligent response to threats (Microsoft Security, 2023[47]). As SIEM solutions store and retain logs, they allow cyber professionals to investigate security incidents, perform forensic analysis, and trace the root causes of breaches or unauthorised activities. This information is vital for understanding the nature of the incident, implementing necessary remediation measures, and preventing future occurrences. Finally, SIEM helps organisations comply with regulatory requirements by providing log collection, retention, and reporting capabilities. It enables cyber professionals to generate compliance reports and demonstrate adherence to industry-specific regulations and standards.

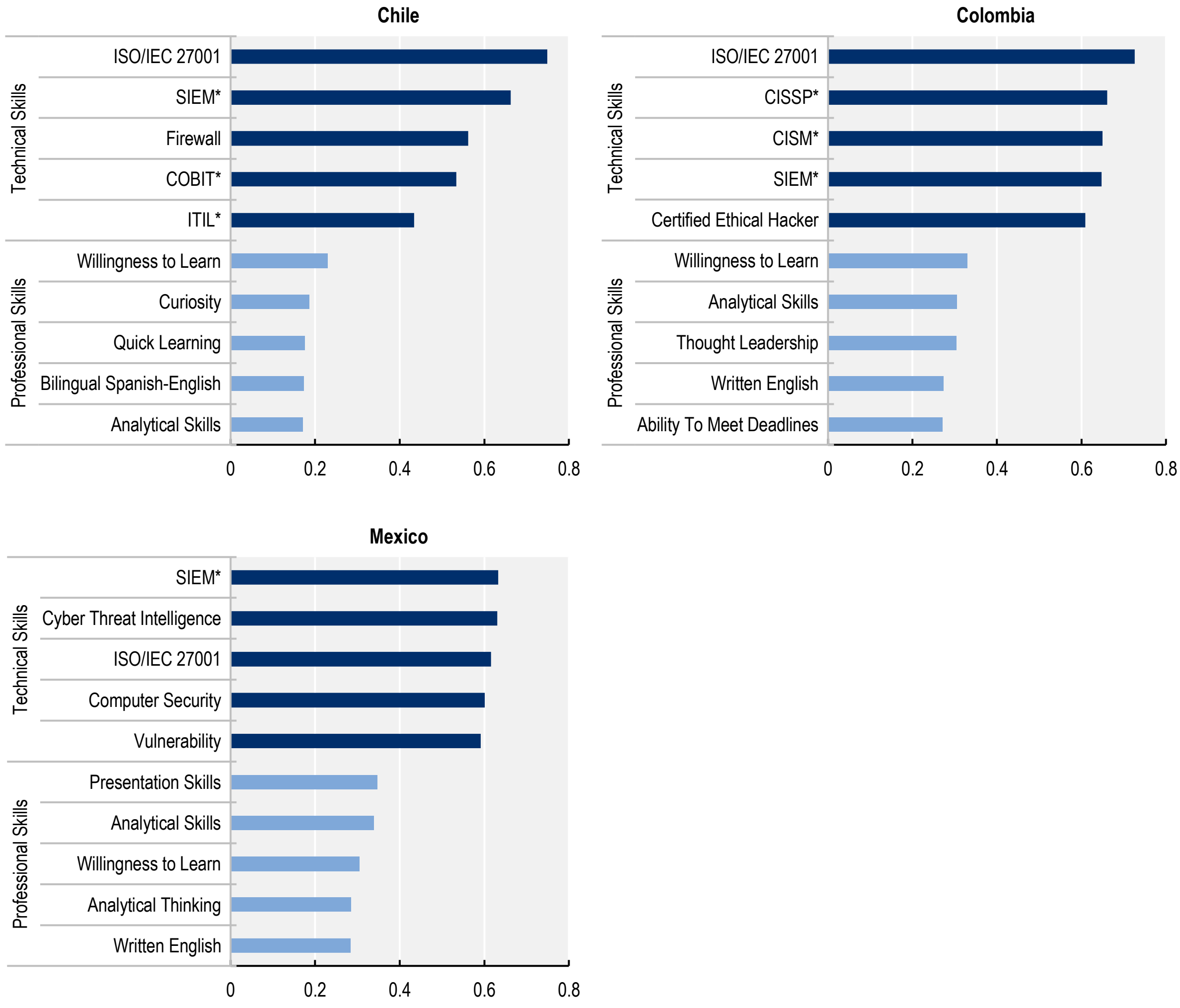
While some cyber security skills requirements are common across countries, others are more specific to the demands of employers in each one of them. The analysis of OJPs in Chile reveals, for instance, that employers put significant emphasis on standards or frameworks for IT service management and IT governance, such as the Control Objectives for Information and Related Technology (COBIT) framework and the Information Technology Infrastructure Library (ITIL). For instance, COBIT is a set of procedures, a roadmap, that helps organisations ensure that their IT processes are running smoothly and aligned with the organisation's needs. These frameworks, although broader in scope, include strategies for risk management and information security relevant for cyber security professionals. This finding is, to some extent, similar to what is observed in the five Anglophone countries analysed in a previous report: Australia, Canada, New Zealand, the United Kingdom and the United States (OECD, 2023[8]); where specialised cyber security frameworks such as the NIST Cybersecurity Framework (NIST CSF), TOGAF, or OWASP were among the most relevant skills required in job postings (Table 2.2 provides more detail on these frameworks).

Results for Colombia indicate that employers in this country explicitly mention cyber-related certifications as a key requirement in prospective candidates, which target mainly highly experience individuals. Three out of the five most relevant keywords extracted from cyber-related OJPs in Colombia are, in fact, certifications: Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), and Certified Ethical Hacker (CEH). Apart from the specific abilities and competencies certified by each of these certificates, it is worth noting that acquiring CISM or a CISSP certification requires a minimum of five years of relevant experience, while CEH requires two years. This finding suggests that employers in Colombia use certifications as a tool to signal their requirements for very specialised skills and experienced profiles in cyber security. The use of certification may be more relevant and useful in Latin American countries than in other countries (see OECD (2023[8])) as most of these countries have not implemented skills frameworks or guidelines that help employers to map workers profiles to their business needs.

Mexico shows a relatively more varied demand for skills across job postings for cyber security professionals. Apart from ISO/IEC 27000 and SIEM, Mexican employers are also likely to demand knowledge of cyber threat intelligence and computer security. The latter is a broad field gathering all those different systems and policies designed to protect the confidentiality and privacy of information processed and stored on a computer. There are four main types of computer security depending on the physical or digital infrastructure, namely, application, information, network and endpoint security (Berkeley Extension, 2023[48]). Cyber threat intelligence is a key component of security systems referring to a set of techniques, tactics and procedures aimed to prevent and mitigate cyber attacks in an organisation's network (Fortinet, 2023[49]).

Figure 2.4. Skill bundle demands in the cyber security profession

Skills with the highest relevance for the cyber security profession in 2022 (closer to 1 = more relevant)



Note: The relevance scores are derived from the semantic analysis of online job postings for each country in 2022. The closer the score to 1, the more relevant the skill for the cyber security occupation in the country at hand. For more details on the methodology see Annex 2.A * SIEM: Security Information and Event Management, CISSP: Certified Information Systems Security Professional, CISM: Certified Information Security Manager, COBIT: Control Objectives for Information and Related Technologies and ITIL: Information Technology Infrastructure Library.
Source: OECD calculations based on Lightcast data.

As in other occupations, along with technical skills, cyber security professionals also need professional/transversal skills, for example to communicate procedures and strategies and to convey technical messages and concepts. Results in Figure 2.4 indicate that transversal skills are typically less relevant than technical skills in cyber security job postings.[12] Among the most relevant transversal skills, Chile, Colombia and Mexico share three: analytical skills, willingness to learn, and English (more precisely, the skills keywords “written English” in Colombia and Mexico, and “bilingual Spanish-English” in Chile).

The enhancement of English language proficiency stands as a crucial factor in mitigating the workforce cyber security gap in Latin America. This region is predominantly marked by low levels of English competency, both in oral and written forms. Particularly, countries like Mexico and Colombia exhibit some of the most substantial deficiencies in English proficiency within the region[13] (see Education First (2022[50])). This proficiency gap creates significant obstacles in the cultivation of cyber security skills, given that relevant training materials, industry standards, and certifications are primarily in English. As a result, organisations often struggle when attempting to implement cutting-edge cyber security tools and technologies.

As explored in Chapter 3, potential short-term solutions could include offering cyber security training in local languages or providing translation services (for instance, those powered by AI translation tools). This approach could help to lower the barriers to accessing cyber security education and resources. Nonetheless, for a more sustainable solution, long-term strategies should focus on fostering English language learning, thereby increasing English proficiency levels in Latin America. By increasing English proficiency, not only can Latin America close its cyber security gap, but it can also unlock wider economic, cultural, and educational opportunities. This, in turn, will strengthen Latin American countries' global competitiveness and enhance its ability to tackle modern digital challenges.

Often, employers in LATAM put also high emphasis on candidates that are "willing to learn" within the cyber security profession. Candidates of this type usually tend to look for new learning opportunities and developing skills to improve their work performance by searching for training, among other strategies (Indeed, 2023[51]). In the case of cyber security, results highlight that a rapidly evolving cyber security landscape requires workers to be open and ready to keep learning new concepts and technologies throughout their professional career.

Results in Figure 2.4 also show that employers seek candidates with strong analytical skills. Critical thinking, problem solving, logical reasoning and creativity help individuals to analyse topics or problems, enabling them to propose complex ideas and effective solutions (Indeed, 2023[52]). As cyber threats continue to advance in complexity, it becomes imperative for professionals to possess abilities to analyse and interpret vast amounts of data efficiently. This expertise enables them to identify patterns and detect anomalies that may indicate potential security breaches or vulnerabilities. With the ever-increasing frequency and sophistication of cyber attacks, cultivating strong analytical skills within the cyber security workforce in Latin America is vital to safeguarding the region's technological infrastructure and improving its cyber resilience.

When comparing these results to those obtained for the five Anglophone countries examined in a previous report (OECD, 2023[8]), the analysis show that employers in all countries prioritise candidates with analytical skills, such as problem solving, critical thinking and strategic thinking, among professional/transversal skills. In the case of Anglophone countries, results showed that employers in those countries were also placing high importance on communication and persuasion skills, while these traits are less prominent in OJPs in LATAM countries. Communication and persuasion skills play an important role facilitating interaction between cyber security teams, other organisational departments, and external clients, especially when explaining technical concepts to non-technical stakeholders. These skills are particularly important in cyber security managerial roles, but data show that fewer of these job postings are currently published in Latin American countries compared to more technologically advanced countries (see also (OECD, 2023[8])).

Box 2.6. Using machine learning to assess the relevance of skills in cyber security occupations

Recent advances in machine learning techniques led to the development of language models which have the objective of understanding the complex relationships between words (their semantics) by deriving and interpreting the context those words appear in. Language models (in particular Natural Language Processing- NLP- models) interpret text information by feeding it to machine learning algorithms that derive the logical rules to interpret the semantic context in which words appear.

NLP models are therefore better suited for the analysis of text information. As such, they are used for the analysis of OJPs in this section of this report. These algorithms allow the calculation of semantic similarity measures between skills and occupations. Skills that are more semantically similar to a certain occupation are interpreted as being more 'relevant' to the occupation (see Annex 2.A for methodological details).

The demand for cyber security frameworks/standards in online job postings

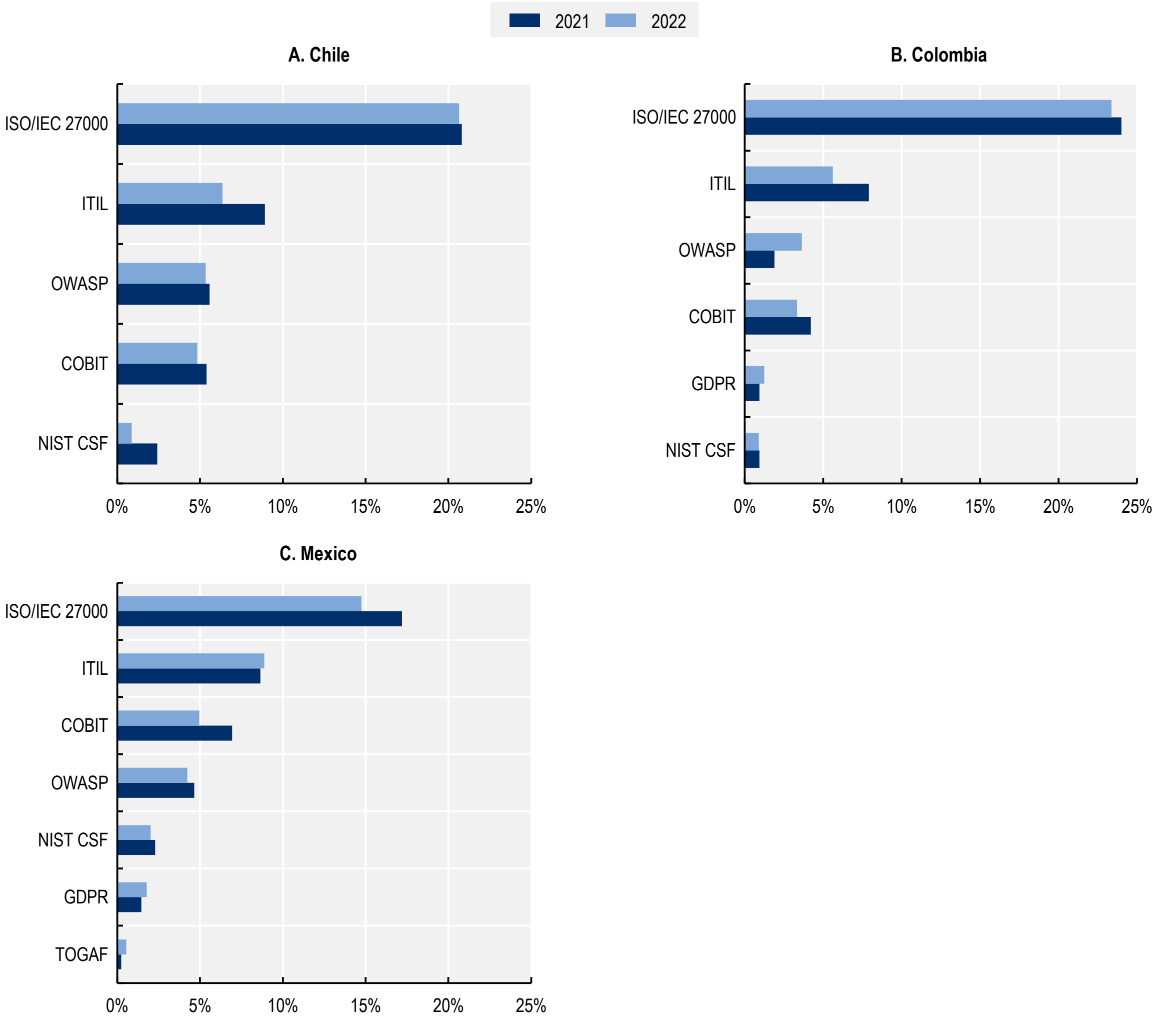
In the rapidly evolving landscape of cyber security, the implementation of well-established frameworks, as well as the adherence to industry standards, play a significant role in ensuring effective cyber security practices. This section explores in more detail the demand in Chile, Colombia and Mexico for cyber security frameworks such as NIST CSF, ITIL and COBIT, and standards such as the ISO/IEC 27000. These frameworks and standards provide essential guidance, best practices, and a common language for organisations and professionals, enabling them to establish comprehensive cyber security strategies, mitigate digital security risk, and enhance overall cyber security resilience.

Adherence to cyber security standards, such as ISO/IEC 27000, is crucial for the cyber security strategy of Latin American organisations. Figure 2.5 shows that this is the most mentioned standard in cyber security OJPs in 2022, ranging from 15% of the total number of OJPs advertised in Mexico during that year to 25% in Colombia. A description of this standard is provided in the previous subsection. It is worth noting that the ISO/IEC 27000 standard enables Latin American organisations to adopt internationally recognised best practices, enhance their credibility in the global market, and demonstrate their commitment to protecting sensitive information.

In addition to the ISO/IEC 27000 standard, cyber security frameworks are vital in the Latin American cyber security sector due to their ability to provide structured approaches and methodologies for addressing cyber security threats. These frameworks offer organisations a systematic and well-defined set of processes, practices, and controls that can be tailored to their specific needs and industry. Compliance with most of the frameworks listed in Figure 2.5 is voluntary. An exception is the EU General Data Protection Regulation (GDPR), for which compliance is compulsory for companies selling products/services in the European Union (GDPR EU, 2022[53]). Table 2.2 provides a brief description of each framework/standard listed in Figure 2.5.

Figure 2.5. Demand for cyber security standards/frameworks

Mentions of each item as a percentage of the total number of cyber security OJPs per year



Note: See Table 2.2 to explore a basic description on cyber security standards/frameworks.
Source: OECD calculations based on Lightcast data.

The Information Technology Infrastructure Library (ITIL) is a widely adopted framework for IT service management (Axelos, 2023[54]). In Mexico nearly 10% of the OJPs advertised in 2022 mention ITIL, and this proportion is slightly above 5% in Chile and Colombia. Although ITIL does not specifically focus on cyber security, it provides valuable guidance for organisations in managing their IT services. By incorporating ITIL into their cyber security practices, organisations can establish robust incident/event management processes, ensure proper access management and align IT security management efforts with overall IT service management objectives (Coursera, 2023[55]).

The NIST CSF is less common in cyber security OJPs in 2022, less than 3% of OJPs mentioning it. A surprising result given the international relevance of this framework as a tool for cyber security risk management. The NIST CSF provides a flexible framework consisting of five core functions: Identify, Protect, Detect, Respond, and Recover, that help organisations assess and improve their cyber security posture. Even though this framework was specifically designed for the United States, it has been adopted as part of the national cyber security strategies of different countries, such as the United Kingdom, Italy, Switzerland and Uruguay (OAS & AWS, 2019[56]). In this line, a previous report (OECD, 2023[8]) shows the high relevance of the NIST CSF among technical skills in Canada, the United Kingdom and the United States.

While frameworks as the NIST CSF could serve as valuable resources for organisations in Latin America aiming to enhance their cyber resilience, their widespread adoption in the region encounters certain challenges. These challenges include the need for commitment from senior management to adopt a cyber security strategy, the establishment of an organisational risk culture and tackling the scarcity of skilled professionals to lead the implementation process (OAS & AWS, 2019[56]). Overcoming these obstacles is essential to effectively leverage frameworks/standards' guidance, promote best practices, and foster collaboration, ultimately bolstering cyber security efforts in Latin America.

Table 2.2. Standards/frameworks mentioned in OJPs from Chile, Colombia and Mexico

Name	Acronym	Description
International Organization for Standardization and International Electrotechnical Commission 27 000 standards	ISO/IEC	The ISO/IEC 27000 standards comprise requirements, guidelines and best practices for information security management. Specifically, OJPs collected refer to the standards ISO/IEC 27001 (Information Security Management System) and ISO/IEC 27002 (information security control objectives).
Information Technology Infrastructure Library	ITIL	Framework including best practices for IT service management and customer experience. ITIL includes provisions for security management, including incident management and access management guidance.
Open Web Application Security Project	OWASP	Open-community contributions to improve web security with guidance, standards, open-source tools and technologies to help security professionals create trusted applications.
Control Objectives for Information and Related Technology	COBIT	This framework helps organisations to manage information technology (IT) governance based on guidelines and best practices. It aims to align IT with business goals, manage digital security risk as well as improve efficiency
National Institute of Standards and Technology Cybersecurity Framework	NIST CSF	The NIST Cybersecurity Framework is a set of guidelines for managing and reducing cyber security risk. It helps organisations identify, protect, detect, respond to, and recover from cyber attacks.
General Data Protection Regulation	GDPR	The GDPR is a regulation that sets guidelines for the collection, processing, and storage of personal data for citizens of the EU. It also applies to companies outside the EU that collect, process or store personal data of individuals located in the EU.
The Open Group Architecture Framework	TOGAF	TOGAF is a framework used by enterprises as a standard for designing and implementing enterprise IT architecture. It aligns IT systems with business goals and objectives.

Source: OECD elaboration based on International Electrotechnical Commission (2023[57]), ISO/IEC 27000 series, https://syc-se.iec.ch/deliveries/cybersecurity-guidelines/security-standards-and-best-practices/iso-27000-series/; The Open Group (2022[58]), The TOGAF® Standard, https://www.opengroup.org/togaf; OWASP (2022[59]), https://owasp.org/about/; NIST (2022[60]), NIST Cybersecurity Framework, https://www.nist.gov/cyberframework/getting-started; ISACA (2019[61]), COBIT: An ISACA Framework, https://www.isaca.org/resources/cobit; Coursera (2023[55]), What Is ITIL?, https://www.coursera.org/articles/what-is-itil; and General Data Protection Regulation (2022[53]), Does the GDPR apply to companies outside of the EU?, https://gdpr.eu/companies-outside-of-europe/.

The demand for cyber security certifications

The results depicted in Figure 2.4 indicate a significant emphasis on certifications in cyber security OJPs. This is particularly evident in Colombia, where the relevance of certifications for the cyber security profession is very high compared to other skill requirements. In Mexico, certifications such as CISSP and CISM are also very relevant for cyber security professionals (relevance scores above 0.5), suggesting that they are usually key requirements used by employers wanting to hire. In Chile, however, relevance scores are low (slightly above 0.3). These values imply that Chilean employers may not prioritise certifications to the same extent as their counterparts in the other two countries when hiring cyber security professionals.

This result also highlights how certifications can represent a useful tool to provide a standardised measure of candidates' knowledge and skills in highly specialised areas such as cyber security. In Latin America, in particular, where the cyber security industry is still developing and evolving, certifications can serve as a common language to assess qualifications and enhance professional credibility of cyber security workers.

Taking a closer look at the frequency with which cyber-related certifications are mentioned in job advertisements across each of the three Latin American countries, Figure 2.6 reveals a varied pattern. Certifications are mentioned in less than 5% of the cyber security OJPs in Chile. This proportion is comparatively lower than that observed in Mexico and Colombia, where the most commonly mentioned certifications appear in approximately 10% of cyber security OJPs. Furthermore, the certifications most frequently mentioned in Mexico and Colombia typically target experienced professionals, as they often require more than five years of relevant work experience, as detailed in Table 2.3.

CISSP, for instance, is one of the certifications most typically mentioned in OJPs for cyber security professionals across the three countries analysed in this report. Approximately 10% of OJPs in Colombia and Mexico mentioned this certification. CISSP is widely recognised as a standard for information security professionals and demonstrates expertise in various domains, including security and risk management, asset security, and communication and network security. This certification requires at least five years of experience and a four-year college degree. It is granted to professionals with a strong foundational and comprehensive knowledge of cyber security principles, making it crucial in managerial or leadership roles.

The Certified Information Security Manager (CISM) is another certification which shows a large number of mentions. CISM validates a professional's expertise in managing and overseeing information security programmes, governance and risk management. With the increasing complexity and frequency of cyber threats, organisations recognise the need for professionals who can develop and implement effective security strategies. The CISM is aimed at experienced workers with a minimum of five years of experience in information security management. This certification indicates a candidate's ability to align security initiatives with organisational objectives, making them valuable assets in protecting sensitive information.

Finally, the demand of the Certified Ethical Hacker (CEH) certification in OJPs experienced growth in Colombia, from 4.2% in 2021 to 6.3% in 2022. Conversely, the mentions of this certification decreased in Chile and Mexico. The CEH is given by the EC-Council and aimed at mid-level professionals with at least two years of experience interested on demonstrating experience as an ethical hacker. Ethical hacking involves assessing systems and networks for vulnerabilities, enabling organisations to proactively identify and address security weaknesses. With the rise of cyber attacks and the importance of proactive security measures, professionals with CEH certifications are sought to strengthen an organisation's defence mechanisms. Ethical hackers play a crucial role in conducting penetration testing, vulnerability assessments, and security audits, thereby helping organisations enhance their cyber security posture.

While the results highlight the importance placed by employers on using some certifications, the analysis also suggests that employers in the region could benefit from using a much wider (and more nuanced) range of cyber security certifications to select candidates, especially when looking to hire workers mid- and entry-level positions. The most requested certifications discussed above, in fact, are typically obtained only by very experienced workers, while employers use them also in job postings for entry-level positions.

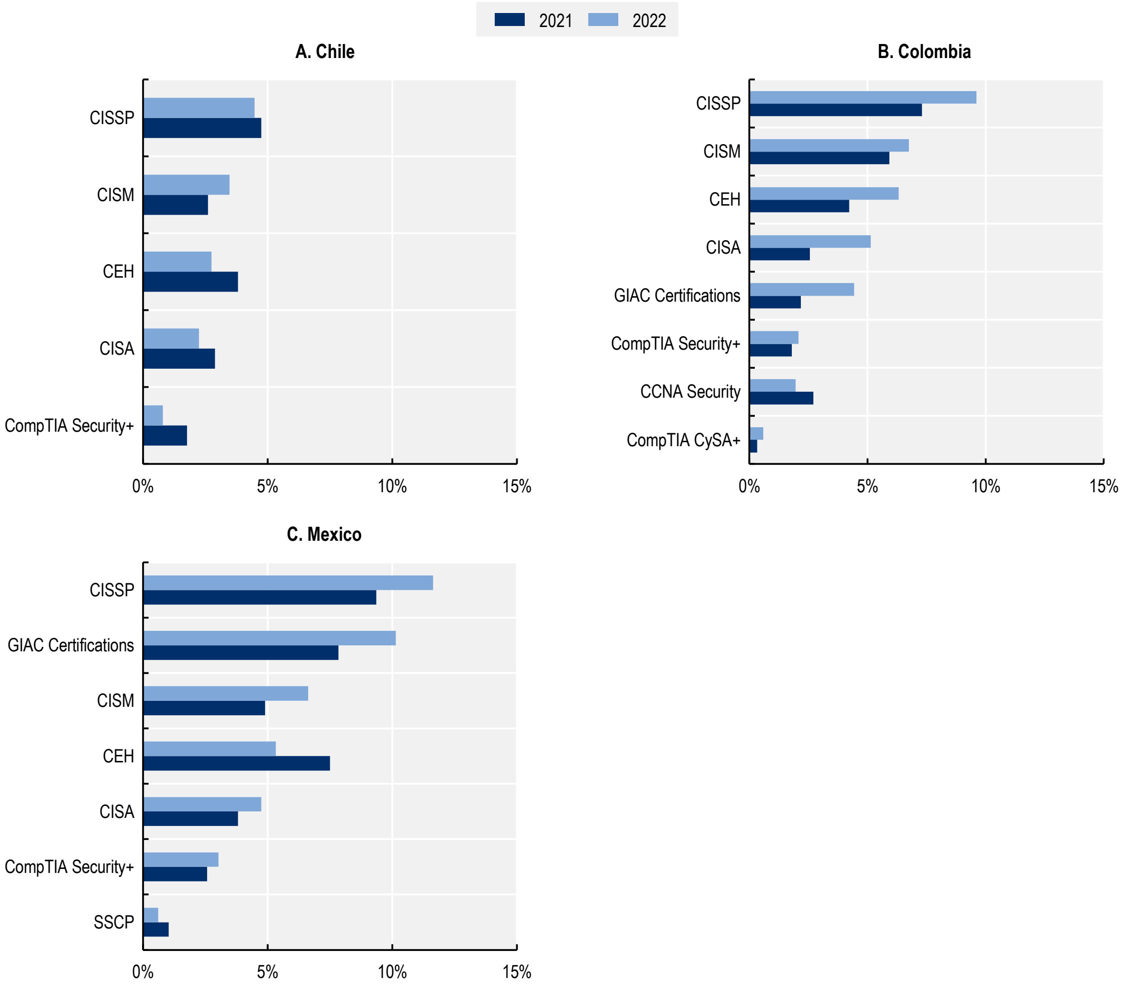
In the Latin American context, in particular, this misalignment becomes apparent in the disparity between the positions that organisations aim to fill and the certification prerequisites they impose. According to the Organization of American States and CISCO, many Latin American organisations seek entry-level cyber security professionals, yet simultaneously demand certifications such as CISSP, which typically mandate a minimum of five years of relevant work experience (OAS & CISCO, 2023[17]). This discrepancy between the desired job level and certification requirements further complicates the efficient matching of talent to available positions in the region's cyber security workforce.

This mismatch creates obstacles for both job seekers and employers. Job seekers who possess the necessary technical skills and knowledge for entry-level positions may be deterred from applying due to the certification requirements. Conversely, employers may face difficulties in finding candidates who meet the certification prerequisites, leading to prolonged vacancies and talent shortages.

This result also suggests the need for reinforcing the awareness amongst employers about a more varied and nuanced ecosystem of available certifications in the market, as many employers may remain unaware of their existence or value.

Figure 2.6. Demand for cyber security certifications

Mentions of each item as a percentage of the total number of cyber security OJPs per year



Note: See Table 2.3 to explore basic information about the certifications required in OJPs.
Source: OECD calculations based on Lightcast data.

Table 2.3. Certifications mentioned in OJPs from Chile, Colombia and Mexico

Name	Acronym	Provider	Experience
Certified Information System Auditor	CISA	ISACA	+ 5 years
Certified Information Security Manager	CISM	ISACA	+ 5 years
Certified Information Systems Security Professional	CISSP	(ICS)2	+ 5 years
GIAC Certified Forensics Analyst	GCFA	GIAC	+ 5 years*
CompTIA CySA+	-	CompTIA	+ 4 years
Certified Ethical Hacker	CEH	EC-Council	+ 2 years
Cisco Certified Network Associate Security	CCNA Security	CISCO	+ 1 year
Systems Security Certified Practitioner	SSCP	(ICS)2	+ 1 year
CompTIA Security+	-	CompTIA	0 years
GIAC Certified Incident Handler	GCIH	GIAC	0 years
GIAC Certified Intrusion Analyst	GCIA	GIAC	0 years
GIAC Security Essentials Certification	GSEC	GIAC	0 years

Note: * The GIAC web page does not specify the experience required for this certificate, however, it is designed for experienced forensic analysts.
Source: OECD elaboration based on Coursera (2023[62]), What Is the CCNA?, https://www.coursera.org/articles/what-is-the-ccna; Coursera (2023[63]), Popular Cybersecurity Certifications, https://www.coursera.org/articles/popular-cybersecurity-certifications; Forbes (2023[64]), https://www.forbes.com/advisor/education/best-cyber-security-certifications/; GIAC (2023[65]), https://www.giac.org/certifications/.

There are several ways to address this issue. On the one hand, employers should carefully evaluate the specific skills and experience needed for entry-level positions and ensure that the skills and/or certification requirements are reasonable and realistic for candidates at that stage of their careers. Additionally, employers can play an active role in supporting their employees' professional growth by providing on-the-job training and certification sponsorship.[14] This approach allows individuals to gain the necessary experience and skills while working, enabling them to progress in their careers and meet certification requirements over time. For instance, Colombia through the "Talento Digital" programme which target enterprises to support cyber security skills development of IT technical teams (see Chapter 3). By investing in their employees' development and supporting their pursuit of certifications, employers can build a skilled workforce and retain talent within their organisations.

The adoption of cyber security skills frameworks is a cornerstone for determining which skills are relevant in each role at different levels of experience. Countries promoting cyber security skills frameworks gather insights from the academia, industry and the government in order to create a comprehensive structure of roles and skills that enable organisations to accurately identify the profiles that are most relevant to their information security areas. Some examples of these frameworks are the Cyber Security Body of Knowledge (CyBOK) in the United Kingdom, the European Cybersecurity Skills Framework (ECSF) and the U.S. National Initiative for Cybersecurity Education (NICE) Framework (see Box 2.7). Other countries, such as Canada, has adapted the NICE Framework to their national labour market to create a national skills framework (for more detail see Government of Canada (2023[66])).

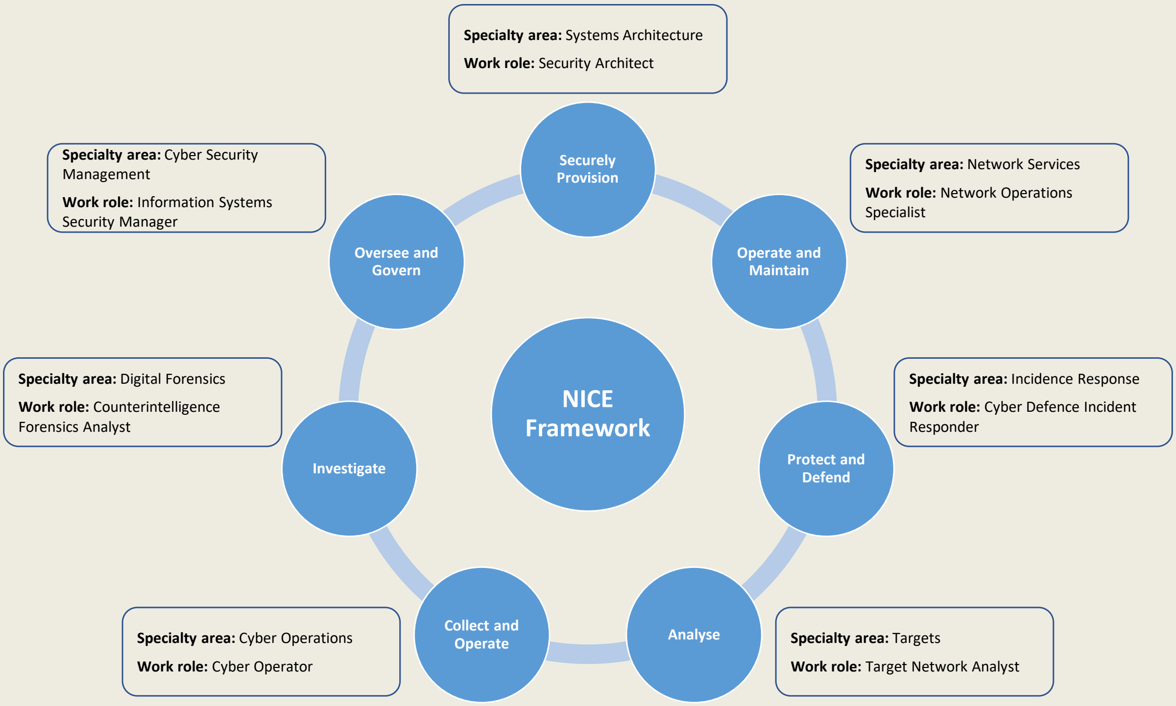
Skills frameworks contribute to a better alignment between skills demand and education/training providers, which brings consistency, relevance, and standardisation to the profession. For example, CompTIA and GIAC certificates are aligned with the NICE Framework, which helps employers to identify the skills they need and support targeted training and career development. Connecting certifications with skills frameworks help the cyber security profession to evolve in line with industry needs and ensure a skilled and competent workforce capable of effectively addressing cyber security challenges.

By implementing these strategies, employers in Latin America can attract a broader pool of qualified candidates, including those at the entry-level, while ensuring that certifications remain a valuable indicator of skills and competence in the cyber security field. This approach also promotes a more inclusive and accessible talent pipeline, strengthening the cyber security workforce, and contributing to the overall growth and resilience of the industry in the region.

Box 2.7. Categorising roles and skills in cyber security: The NICE Cybersecurity Framework

The NICE framework offers a comprehensive and structured approach to describing the various tasks performed within the cyber security profession in the United States. It outlines the specific knowledge and skills needed to carry out these tasks effectively based on four main hierarchical components: Categories (blue bubbles in Figure 2.7); Specialty areas; Work roles; and Knowledge, skills and abilities (KSAs). By utilising the NICE framework, organisations can establish a common language and understanding when defining cyber security skills and roles, thereby reducing ambiguity and ensuring better alignment between job requirements and candidate qualifications.

Figure 2.7. NICE Cybersecurity Workforce Framework


Specialty area: Systems Architecture
Work role: Security Architect
Specialty area: Cyber Security Management
Work role: Information Systems Security Manager
Specialty area: Network Services
Work role: Network Operations Specialist
Securely Provision
Oversee and Govern
Operate and Maintain
NICE Framework
Specialty area: Digital Forensics
Work role: Counterintelligence Forensics Analyst
Specialty area: Incidence Response
Work role: Cyber Defence Incident Responder
Investigate
Protect and Defend
Collect and Operate
Analyse
Specialty area: Cyber Operations
Work role: Cyber Operator
Specialty area: Targets
Work role: Target Network Analyst

Note: This figure provides one example of the specialty areas and work roles linked to each main category in the NICE Framework.
Source: OECD based on National Initiative for Cybersecurity Careers and Studies (2023[30]), NICE Framework, https://niccs.cisa.gov/workforce-development/nice-framework.

Implementing frameworks like NICE enables organisations to go beyond generic job titles and delve into the specific responsibilities and competencies associated with cyber security positions. This facilitates more accurate job descriptions, allowing employers to attract candidates with the right skill sets for the targeted roles.

Moreover, frameworks like NICE enhance the recruitment and selection process by enabling organisations to identify and assess candidates based on a standardised set of knowledge and skills. This not only streamlines the hiring process but also ensures that individuals possess the necessary capabilities to meet the organisation's cyber security needs effectively.

Countries such as Australia, Canada, Singapore and Japan have adapted the NICE Framework to their own cyber security skills programmes, highlighting the benefits of this frameworks for creating a skilled cyber security workforce. However, none of the Latin American countries has formally adopted this initiative (OAS & AWS, 2020[67]).

References

(ISC)2 (2022), *2022 Cybersecurity Workforce Study*, https://www.isc2.org/Research/Workforce-Study (accessed on April 2023). [1]

Axelos (2023), *ITIL® 4: the framework for the management of IT-enabled services*, https://www.axelos.com/certifications/itil-service-management/ (accessed on June 2023). [54]

Banco Mundial (2023), *Chile Panorama general*, https://www.bancomundial.org/es/country/chile/overview (accessed on May 2023). [14]

Berkeley Extension (2023), *What is computer security?*, https://bootcamp.berkeley.edu/blog/what-is-computer-security/#1661270174332-b8c3d196-c6e9. [48]

Cámara de Diputados (2023), *Nota No. 6328 Ingresan iniciativa de la Ley Federal de Ciberseguridad a la Cámara de Diputados*, https://comunicacionsocial.diputados.gob.mx/index.php/notilegis/ingresan-iniciativa-de-la-ley-federal-de-ciberseguridad-a-la-camara-de-diputados (accessed on May 2023). [25]

Cammeraat, E. and M. Squicciarini (2021), “Burning Glass Technologies’ data use in policy-relevant analysis: An occupation-level assessment”*, OECD Science, Technology and Industry Working Papers*, No. 2021/05, OECD Publishing, Paris, https://doi.org/10.1787/cd75c3e7-en. [4]

Council of Europe (2022), *Chile: Status regarding Budapest Convention*, https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/chile (accessed on May 2023). [12]

Council of Europe (2001), *Convention on Cybercrime*, https://rm.coe.int/1680081561 (accessed on June 2023). [15]

Coursera (2023), *10 Popular Cybersecurity Certifications [2023 Updated]*, https://www.coursera.org/articles/popular-cybersecurity-certifications (accessed on May 2023). [63]

Coursera (2023), *What Is ITIL? A Beginner’s Guide to the ITIL Process*, https://www.coursera.org/articles/what-is-itil (accessed on May 2023). [55]

Coursera (2023), *What Is the CCNA? An Entry-Level Networking Certification*, https://www.coursera.org/articles/what-is-the-ccna (accessed on May 2023). [62]

CSIRT (2021), *Sobre 2.300 millones de intentos de ataques recibió Chile en 2020, de acuerdo con Fortinet*, https://www.csirt.gob.cl/noticias/sobre-2-300-millones-de-intentos-de-ataques-recibio-chile-en-2020-de-acuerdo-con-fortinet/ (accessed on May 2023). [11]

DANE (2018), *Censo Nacional de Población y Vivienda 2018*, https://www.dane.gov.co/index.php/estadisticas-por-tema/demografia-y-poblacion/censo-nacional-de-poblacion-y-vivenda-2018 (accessed on May 2023). [33]

Education First (2022), *EF English Proficiency Index 2022*, https://www.ef.com/ca/epi/ (accessed on May 2023). [50]

European Parliament (2021), *The informal economy and coronavirus in Latin America*, https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690587/EPRS_BRI(2021)690587_EN.pdf (accessed on June 2023). [35]

Fadic, M. et al. (2019), "Classifying small (TL3) regions based on metropolitan population, low density and remoteness"*, OECD Regional Development Working Papers*, No. 2019/06, OECD Publishing, Paris, https://doi.org/10.1787/b902cc00-en. [71]

Forbes (2023), *Best Cybersecurity Certifications: What Do You Need To Know?*, https://www.forbes.com/advisor/education/best-cyber-security-certifications/ (accessed on May 2023). [64]

FortiGuard Labs (2023), *Comunicado de prensa: Fortinet informa que América Latina fue el objetivo de más de 360 mil millones de intentos de ciberataques en 2022*, https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2023/fortiguard-labs-reports-destructive-wiper-malware-increases-over-50-percent (accessed on May 2023). [23]

Fortinet (2023), *2023 cyber security skills gap*, https://edu.arrow.com/media/0pld3mup/2023-cybersecurity-skills-gap-report.pdf. [2]

Fortinet (2023), *What is Cyber Threat Intelligence?*, https://www.fortinet.com/resources/cyberglossary/cyber-threat-intelligence (accessed on May 2023). [49]

GDPR EU (2022), *Does the GDPR apply to companies outside of the EU?*, https://gdpr.eu/companies-outside-of-europe/ (accessed on May 2023). [53]

GIAC (2023), *GIAC certifications*, https://www.giac.org/certifications/ (accessed on May 2023). [65]

González, N. (2022), *De no tomar acciones, Colombia tendría déficit de 112.000 desarrolladores en 2025*, https://www.larepublica.co/alta-gerencia/de-no-tomar-acciones-colombia-tendria-deficit-de-112-000-desarrolladores-en-2025-3440141 (accessed on June 2023). [43]

Government of Canada (2023), *The Canadian cyber security skills framework*, https://www.cyber.gc.ca/en/education-community/academic-outreach-cyber-skills-development/canadian-cyber-security-skills-framework#defn-cyber-security (accessed on May 2023). [66]

Government of Mexico (2022), *Fabricación de Componentes Electrónicos*, https://www.economia.gob.mx/datamexico/es/profile/industry/semiconductor-and-other-electronic-component-manufacturing?redirect=true (accessed on 12 May 2023). [37]

Government of Mexico (2017), *National Cyber Security Strategy*, https://www.gob.mx/cms/uploads/attachment/file/399655/ENCS.ENG.final.pdf (accessed on May 2023). [24]

IADB & OAS (2020), *Cybersecurity: Risks, progress, and the way forward in Latin America and the Caribbean*, https://doi.org/10.18235/0002513 (accessed on April 2023). [16]

INAI (2022), *Emite INAI recomendaciones para proteger datos personales ante un crackeo o ciberataque*, https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Comunicado%20INAI-385-22.pdf (accessed on May 23). [22]

Indeed (2023), *How To Demonstrate Your Willingness To Learn at Work*, https://www.indeed.com/career-advice/interviewing/willingness-to-learn (accessed on May 2023). [51]

Indeed (2023), *What Are Analytical Skills? Definition, Examples and Tips*, https://www.indeed.com/career-advice/resumes-cover-letters/analytical-skills (accessed on May 2023). [52]

Indeed (2023), *What Are Financial Advisor Skills? (Definition and Examples)*, https://sg.indeed.com/career-advice/finding-a-job/financial-advisor-skills (accessed on May 2023). [45]

INE (2017), *Censo de Población y Vivienda*, https://www.ine.gob.cl/estadisticas/sociales/censos-de-poblacion-y-vivienda/censo-de-poblacion-y-vivienda (accessed on May 2023). [34]

INEGI (2020), *Censo de Población y Vivienda 2020 - SCITEL*, https://www.inegi.org.mx/app/scitel/Default?ev=9 (accessed on May 2023). [32]

International Electrotechnical Commission (2023), *ISO/IEC 27000 series*, https://syc-se.iec.ch/deliveries/cybersecurity-guidelines/security-standards-and-best-practices/iso-27000-series/ (accessed on May 2023). [57]

International Labour Organization (n.d.), *Updating the International Standard Classification of Occupations (ISCO) - Draft ISCO-08 Group Definitions: Occupations in ICT*, https://www.ilo.org/public/english/bureau/stat/isco/docs/d2434.pdf (accessed on April 2023). [68]

ISACA (2019), *COBIT: An ISACA Framework*, https://www.isaca.org/resources/cobit (accessed on May 2023). [61]

Joint Task Force Transformation Initiative (2018), *Risk management framework for information systems and organizations:*, National Institute of Standards and Technology, Gaithersburg, MD, https://doi.org/10.6028/nist.sp.800-37r2. [29]

Kirk, J. (2018), *Banco de Chile Loses $10 Million in SWIFT-Related Attack*, https://www.bankinfosecurity.com/banco-de-chile-loses-10-million-in-swift-related-attack-a-11075 (accessed on May 2023). [10]

Kirk, J. (2018), *Mexico Investigates Suspected Cyberattacks Against 5 Banks*, https://www.bankinfosecurity.com/mexico-investigates-suspected-cyberattacks-against-banks-a-11008 (accessed on May 2023). [21]

La República (2023), *Recuperación del empleo: un gran reto para 2023*, https://www.larepublica.co/analisis/anif-3478852/recuperacion-del-empleo-un-gran-reto-para-2023-3538890 (accessed on May 2023). [18]

Manca, F. (2023), “Six questions about the demand for artificial intelligence skills in labour markets”*, OECD Social, Employment and Migration Working Papers*, No. 286, OECD Publishing, Paris, https://doi.org/10.1787/ac1bebf0-en. [70]

Microsoft (2023), *ISO/IEC 27001:2022*, https://learn.microsoft.com/en-us/azure/compliance/offerings/offering-iso-27001 (accessed on May 2023). [46]

Microsoft (2022), *Regular Expression Language - Quick Reference*, https://learn.microsoft.com/en-us/dotnet/standard/base-types/regular-expression-language-quick-reference (accessed on April 2023). [69]

Microsoft Security (2023), *What is SIEM?*, https://www.microsoft.com/en-gb/security/business/security-101/what-is-siem (accessed on May 2023). [47]

MinTIC (2020), *CONPES 3995 - Política nacional de confianza y seguridad digital*, https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf (accessed on June 2023). [20]

MinTIC (2016), *CONPES 3854: Política Nacional de Seguridad Digital*, https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf (accessed on May 2023). [19]

Moncayo, M. and S. Guzmán (2022), *All Eyes on Colombia's Tech Sector*, https://theglobalamericans.org/2022/12/all-eyes-on-colombias-tech-sector/ (accessed on May 2023). [39]

NICCS (2023), *Systems Architecture: Security Architect*, https://niccs.cisa.gov/workforce-development/nice-framework/specialty-areas/systems-architecture (accessed on March 2023). [28]

NICCS (2023), *Workforce Framework for Cybersecurity (NICE Framework)*, https://niccs.cisa.gov/workforce-development/nice-framework (accessed on May 2023). [30]

NIST (2022), *NIST Cybersecurity Framework*, https://www.nist.gov/cyberframework/getting-started (accessed on May 2023). [60]

OAS & AWS (2020), *Educación en Ciberseguridad. Planificación del futuro mediante el desarrollo de la fuerza laboral*, https://www.oas.org/es/sms/cicte/docs/20200925-ESP-White-Paper-Educacion-en-Ciberseguridad.pdf. [67]

OAS & AWS (2019), *Marco NIST. Un Abordaje Integral de la Ciberseguridad*, https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf (accessed on May 2023). [56]

OAS & CISCO (2023), *Reporte sobre el desarrollo de la fuerza laboral de ciberseguridad en una era de escasez de talento y habilidades*, https://www.oas.org/es/sms/cicte/docs/Reporte_sobre_el_desarrollo_de_la_fuerza_laboral_de_ciberseguridad_en_una_era_de_escasez_de_talento_y_habilidades.pdf (accessed on April 2023). [17]

OECD (2023), *Building a Skilled Cyber Security Workforce in Five Countries: Insights from Australia, Canada, New Zealand, United Kingdom, and United States*, OECD Skills Studies, OECD Publishing, Paris, https://doi.org/10.1787/5fd44e6c-en. [8]

OECD (2022), *Education at a Glance 2022: OECD Indicators*, OECD Publishing, Paris, https://doi.org/10.1787/3197152b-en. [36]

OECD (2022), *OECD Economic Outlook, Volume 2022 Issue 2*, OECD Publishing, Paris, https://doi.org/10.1787/f6da2159-en. [13]

OECD (2022), *OECD Employment Outlook 2022: Building Back More Inclusive Labour Markets*, OECD Publishing, Paris, https://doi.org/10.1787/1bb305a6-en. [26]

OECD (2022), *Rural Policy Review of Colombia 2022*, OECD Rural Studies, OECD Publishing, Paris, https://doi.org/10.1787/c26abeb4-en. [31]

OECD (2022), *Skills for the Digital Transition: Assessing Recent Trends Using Big Data*, OECD Publishing, Paris, https://doi.org/10.1787/38c36777-en. [40]

OECD (2021), *OECD Skills Outlook 2021: Learning for Life*, OECD Publishing, Paris, https://doi.org/10.1787/0ae365b4-en. [5]

OWASP (2022), *About the OWASP Foundation*, https://owasp.org/about/ (accessed on May 2023). [59]

Paez Jiminez, E. (2023), *Ley de Ciberseguridad en México: nueva agencia, registro y estrategia nacional*, https://dplnews.com/ley-de-ciberseguridad-en-mexico-nueva-agencia-registro-y-estrategia-nacional/ (accessed on June 2023). [27]

Ruiz Tagle-Vial, P. and D. Álvarez-Valenzuela (2020), *Building Cybersecurity Capacity: Challenges for Post-Secondary Education in Latin America and the Caribbean*, https://doi.org/10.18235/0002513 (accessed on April 2023). [3]

Taplin, S. (2022), *Mexico Is Flooded With Top Software Development Talent*, https://www.forbes.com/sites/forbestechcouncil/2022/04/13/mexico-is-flooded-with-top-software-development-talent/?sh=467ad61f4960 (accessed on June 2023). [42]

Tecla (2023), *Nearshore Software Development in Mexico Report*, https://www.tecla.io/blog/nearshore-software-development-in-mexico-report (accessed on June 2023). [41]

The Open Group (2022), *The TOGAF® Standard, 10th Edition*, https://www.opengroup.org/togaf (accessed on May 2023). [58]

UNESCO - UNEVOC (2023), *UNESCO TVETipedia Glossary: Technical Skills*, https://unevoc.unesco.org/home/TVETipedia+Glossary/lang=en/show=term/term=Technical+skills (accessed on March 2023). [6]

United Nations Statistics Division (2023), *International Merchandise Trade Statistics*, https://comtradeplus.un.org/TradeFlow (accessed on May 2023). [38]

Universidad De Chile (2023), *https://ingenieria.uchile.cl/carreras/4969/ingenieria-civil*, https://ingenieria.uchile.cl/carreras/4969/ingenieria-civil (accessed on June 2023). [44]

UNODC (2017), *Chile's national cybersecurity policy 2017-2022*, https://www.unodc.org/e4j/data/_university_uni_/chiles_national_cybersecurity_policy_2017-2022.html?lng=en (accessed on May 2023). [9]

World Economic Forum (2022), *Global Cybersecurity Outlook 2022*, https://www.weforum.org/reports/global-cybersecurity-outlook-2022/ (accessed on March 2023). [7]

Annex 2.A. Methodological annex

Classifying cyber security jobs using job titles

The online job postings data provided by Lightcast for Latin American countries are mapped to the International Standard Classifications of Occupations (ISCO-08), a four-digit hierarchical classification used to categorise each online job posting in one of the several occupations contained in this structure. However, for the purpose of identifying cyber security job postings, the ISCO-08 lacks granularity. Within the two-digit group "ICT professionals" (25), the four-digit occupation "Database and network professionals not elsewhere classified" (2529) includes occupations performing some tasks related with the cyber security profession, such as "encrypting data transmissions and erecting firewalls", "regulate access to safeguard information" or "performing risk assessments", but it is not limited to this occupation (International Labour Organization, n.d.[68])

In this context, leveraging the text available in the job titles contributes to obtain a more precise classification of cyber security job postings. For this purpose, this report uses a classification strategy based on regular expressions. This concept refers to sequences of characters provided to an algorithm to match patterns in a text (Microsoft, 2022[69]). The first row in Annex Table 2.A.1 shows the regular expressions selected for classifying the online job postings. These expressions are the result of evaluating hundreds of the most frequent bigrams (all the possible combinations of two words) extracted from the job titles available in English and Spanish. After a manual review of the results for each country, additional expressions were necessary to exclude some jobs misclassified in the first stage, as shown in the second row in Annex Table 2.A.1.

Annex Table 2.A.1. Regular expressions for classifying cyber security jobs

Regular expressions are sequences of characters used to match a pattern in a text.

<table>
<tr><th>Group</th><th>Regular expressions</th></tr>
<tr><td>Expression for <b>classifying</b> job postings as cyber security jobs</td><td>“\\b(?i)redes y seguridad\\b”, “(?i)arcsight”, “(?i).*ciber.*”, “(?i).*cyber.*”, “(?i)endpoint”, “(?i)fortinet”, “(?i).*info.*seguridad.*”, “(?i).*protecc.*datos.*”, “(?i).*seguridad.*iinfo.*”, “(?i).*seguridad.*info.*”, “(?i)application(?=‘.*security).*”, “(?i)arquitecto(?=‘.*seguridad).*”, “(?i)data(?=‘.*(protection|security)).*”, “(?i)datos(?=‘.*seguridad).*”, “(?i)information(?=‘.*protection).*”, “(?i)infraestructura(?=‘.*seguridad).*”, “(?i)infrastructure(?=‘.*security).*”,”(?i)network(?=‘.*security).*”, “(?i)security(?=‘.*(architect|devops|infrastructure|software)).*”, “(?i)seguridad(?=.*(datos|infraestructura|redes)).*”</td></tr>
<tr><td>Expression for <b>excluding</b> job postings from cyber security jobs</td><td>“\\b(?i)ciberliteratura\\b”, “(?i).*cibercaf.*”, “(?i).*day.*”, “\\b(?i)apoyo cyber\\b”, “\\b(?i)proyecto cyber\\b”, “\\b(?i)infonavit\\b”, “\\b(?i)recolector\\b”, “\\b(?i)operario\\b”, “\\b(?i)asistente\\b”, “\\b(?i)apoyo evento\\b”, “\\b(?i)temporada cyber\\b”, “\\b(?i)cyber easy\\b”, “\\b(?i)easy cyber\\b”, “\\b(?i)seguridad privada\\b”, “\\b(?i)guardia de seguridad\\b”</td></tr>
</table>

Source: OECD based on Lightcast data.

Groups of roles within the cyber security profession

Within the cyber security online job postings there is a variety of roles demanded by enterprises. Identifying these roles can be useful to characterise cyber security job markets with more detail than traditional labour markets' data sources. Specifically, job titles are once again a rich source of information useful to extract this feature. However, since job titles do not follow a particular pattern, this report uses an approach based on keywords matches to classify each online job posting in a given role.

In a first stage, this approach leverages the most frequent unigrams (every single word available) or keywords available in job titles from the three countries (Chile, Colombia and Mexico). Based on these words, and on previous reports using this approach (OECD, 2023[8]), four groups of roles are considered: Analysts, Architects and Engineers, Auditors and Advisors, and Managers. In a second stage, this approach assigns different keywords to each group that allows the algorithm to classify each online job postings in the appropriate role. Annex Table 2.A.2 shows the keywords selected for each group, as well as a sample of the job titles classified on each of them. If not classified in one of the groups, job postings are assigned to the category "others".

Annex Table 2.A.2. Groups of cyber security roles

Cyber security groups	Keywords	Sample of job titles
Analysts	Analista, Analyst, Especialista, Specialist, Oficial, Officer, Experto, Expert, Profesional, Professional, Gestor, Associate	Analista de Ciberseguridad, Oficial de Seguridad de la Información, Especialista en Ciberseguridad, Cyber Security Analyst
Architects and Engineers	Ingeniero, Ingeniera, Ing, Engineer, Arquitecto, Arquitecta, Architect, Tecnico, Técnico, Tcnico, Developer, Devops, Desarrollador, Penetration, Tester, Administrador, Administrator, Admin	Ingeniero Ciberseguridad, Arquitecto de Ciberseguridad, Ingeniero de Seguridad Informática, Cyber Security Engineer, Network Security Engineer
Auditors and Advisors	Auditor, Auditora, Consultor, Consultora, Consultant, Asesor, Asesora, Abogado, Abogada, Supervisor, Counsel, Advisor	Auditor de Ciberseguridad, Consultor de Seguridad de la Información, Network Security Advisor, Cyber Security Senior Consultant
Managers	Presidente, President, Gerente, Líder, Lider, Lead, Lder, Leader, Manager, Director, Directora, Executive, Ejecutivo, Chief, Partner, Jefe, Co-ordinador, Co-ordinator, Principal, Head	Jefe de Ciberseguridad, Vice President – Cyber Risk, Gerente producto Ciberseguridad, Co-ordinador De Seguridad Informática, Data Protection Service Operations Manager

Source: OECD based on Lightcast data.

A semantic analysis approach to assess skills relevance

Recent developments in Natural Language Processing (NLP) are useful to leverage the semantic meaning of the information contained in the online job postings. Specifically, a word embedding approach is applied to generate a semantic representation of each word in an *n*-dimensional vector, where each dimension indicates a specific context item. This representation allows for the calculation of mathematical similarity measures to represent the similarity between different skills and professions/occupations. In particular, the approach taken in this report leverages 'Word2Vec', an NLP algorithm developed in 2013 by researchers in Google.

To obtain the most relevant skills for cyber security professionals, the analysis in this report creates a Semantic Skill Bundle Matrix (SSBM) by calculating the cosine similarity index between all possible combinations of skills and professions. The cosine similarity index is based on the cosine of the angle between vector representations of words. When a pair of words are closely related, the angle of their vectors is closed to 0 and the cosine is close to 1. Conversely, when the cosine is negative the words can be related but are opposite in meaning. Specifically, the calculation of the index for occupation A and skill B is:

$$CosSim(A,B) = \frac{(A \cdot B)}{\|A\|\|B\|}$$

Applying this approach is, therefore, possible to assess whether the skill “Excel” is more relevant to the occupation “Economist” or to “Painter”, based on the semantic closeness of these words’ meanings extrapolated from millions of job postings. This is used, in turn, to generate indicators of the relevance of technical and professional skills for cyber security professionals based on the language/semantic analysis of the text contained in the OJPs in each country considered.

Recent OECD work (Manca, 2023[70]) validates the assumption by which semantic similarity scores derived from word embeddings can be used as a measure of skills relevance for each occupation. In particular, the report compares the results of the similarity scores with expert constructed scores available in the O*NET database. It shows that correlation between similarity scores and the O*NET values is positive, strong (0.62) and statistically significant across all possible combinations of occupations and skills.

Annex 2.B. Metropolitan cities versus metropolitan regions

The standard classification of a metropolitan region is a Territorial Level 3 (TL3) region for which more than 50% of its population live in a functional urban area (FUA) of at least 250 000 inhabitants. TL3 regions are smaller territorial regions that together make-up a region at the first administrative tier of subnational government (TL2). In case of Colombia for instance, the TL2 regions are the departments, while the TL3 regions are the provinces/subregions. FUAs consist of cities and their corresponding hinterlands, areas which are close to the cities. (Fadic et al., 2019[71])

The current report, by contrast, uses metropolitan cities to analyse where the demand for cyber security professionals is located. Cities with 250 000 inhabitants or more are designated as metropolitan cities. While metropolitan cities are part of metropolitan regions, a metropolitan region can encompass a larger area. According to the latest censuses there are 71 metropolitan cities in Mexico, 28 in Colombia and 11 in Chile (DANE, 2018[33]; INEGI, 2020[32]; INE, 2017[34]).

Cities are chosen as a reference point, due to the availability of the data on job postings in the Lightcast datasets. The datasets contain information on the TL2 regions: *departamentos* in Colombia; *regions* in Chile; and *estados* in Mexico, and on the cities in which the OJPs are posted. It does not state which TL3 region is linked to each OJP.

Annex 2.C. Related occupations

Annex Table 2.C.1. Overview of digital, engineering, and math-related occupations

Group	Related job name	ISCO codes
1- Computer and data analysts / administrators	Database and network professionals not elsewhere classified	2529
1- Computer and data analysts / administrators	Database designers and administrators	2521
1- Computer and data analysts / administrators	Systems analysts	2511
1- Computer and data analysts / administrators	Systems administrators	2522
1- Computer and data analysts / administrators	Computer network professionals	2523
2-Software developers and programmers	Web and multimedia developers	2513
2-Software developers and programmers	Applications programmers	2514
2-Software developers and programmers	Software developers	2512
2-Software developers and programmers	Software and applications developers and analysts not elsewhere classified	2519
3-ICT technicians	Web technicians	3514
3-ICT technicians	Information and communications technology user support technicians	3512
3-ICT technicians	Information and communications technology operations technicians	3511
3-ICT technicians	Information technology trainers	2356
3-ICT technicians	Computer network and systems technicians	3513
3-ICT technicians	Telecommunications engineering technicians	3522
4- Math related professions	Mathematicians, actuaries and statisticians	2120
4- Math related professions	Statistical, mathematical and related associate professionals	3314
4- Math related professions	Financial and investment advisers	2412
4- Math related professions	Financial analysts	2413
5- Engineers and technicians	Mechanical engineers	2144
5- Engineers and technicians	Engineering professionals not elsewhere classified	2149
5- Engineers and technicians	Civil engineers	2142
5- Engineers and technicians	Industrial and production engineers	2141
5- Engineers and technicians	Telecommunications engineers	2153
5- Engineers and technicians	Electronics engineers	2152

Notes

[1] https://lightcast.io/.

[2] For further details on the methodology, please see Box 2.1 and Annex 2.A. Figure 2.1 presents the number of OJPs (Panel A) and the shares (Panel B) in the demand of four cyber security roles: analysts, architects and engineers, auditors and advisors, and managers.

[3] The demand for cyber security auditors and advisors in Mexico also experienced a significant growth in recent years. Specifically, the demand for professionals in this role expanded by 79% between 2021 and 2022.

[4] According to the "Geographic concentration index of the population in OECD countries, 2019" (OECD, 2022[31])

[5] For more information on the term metropolitan cities and how it relates to the more commonly used classification of metropolitan regions, see Annex 2.B

[6] Out of the OJPs for which the location is known. The share of OJPs without information on the location is 38.8% in Chile, 27.3% in Colombia and 33.9% in Mexico.

[7] Out of the OJPs for which the sector is known, which is 36% of OJPs.

[8] It should be noted that the Lightcast data for LATAM are still experimental and that deduplication of observations can be imperfect. This can affect some of the results by increasing the volume of job postings for some occupations, especially in 2021. The extent of this issue cannot be indicated.

[9] The five groups consist of different jobs at the four-digit ISCO level, which were chosen because of their affinity with algorithms, digital skills and use of (big) data. For a list of all selected occupations and their groups selected see Annex 2.C.

[10] Mexico and the United States, for instance, share a long border and being on the same time zone facilitate smoother communication between headquarters and subsidiaries.

[11] The group of math-related professions is 19.6% of the digital, engineering and math-related OJPs in Chile.

[12] The relevance scores of transversal skills are, by definition, lower than those for technical skills as transversal skills are typically required in a wide range of professions and these skills are not 'core' to any specific job role. That being said, it is interesting to analyse what are the most relevant transversal skills in cyber security professions and how these mix with the most relevant technical skills.

[13] For instance, the Education First English Proficiency Index ranks Chile in a moderate proficiency level, while Colombia and Mexico appear in the low and very low proficiency levels respectively. English language learners in Latin America lag behind other regions due to factors such as uneven access to quality education, lack of teacher training, and absence of public policies promoting language learning. To address this, initiatives could include structured English programmes in schools, professional development for English teachers, and greater accessibility to English language resources.

[14] Certifications can be costly for learners. This economic barrier can limit the ability of potential cyber security professionals to acquire certifications, especially in regions like Latin America, where financial constraints may be more prevalent compared to developed nations.

3 The landscape of cyber security education and training programmes: The case of Colombia

This chapter explores cyber security education and training in Colombia, focusing on preparation for entry-level cyber security roles. It describes the landscape of education and training programmes, current learner profiles, and labour market outcomes. Special attention is dedicated to efforts to create a strong framework for the provision of cyber security programmes, including national strategies for cyber security skills, and efforts to diversify provision within higher education and to tackle teacher shortages. The chapter also looks at access and inclusion, describing challenges and initiatives designed to promote participation in cyber security learning, including among female learners and those from disadvantaged backgrounds.

Introduction: Setting the scene for more effective cyber security skills policies

Chapter 2 highlights the significant and growing demand for cyber security professionals in Latin American countries (LATAM), in particular in Chile, Colombia, and Mexico. This trend reflects the expansion of connectivity, especially in urban areas, the adoption of a broader range of digital technologies, and an increase in remote work opportunities. However, the recent surge in demand for cyber security professionals has not been met with a sufficient supply of trained workers, resulting in shortages that can potentially expose vulnerabilities in cyber security. These shortages are already observed today, as evidenced by research conducted by Fortinet (2023[1]), which indicates that 41% of LATAM organisations surveyed struggle to fill cloud security roles.

This chapter focuses on the Colombian context, providing a detailed overview of its cyber security education and training landscape, along with associated policies to grow and diversify its cyber security workforce. Education and training focused on developing cyber security skills is key to counteract cyber security threats and tackle skill shortages. At the same time, it is essential to have a broader understanding of the population's digital skill capacity, which is a pre-condition to having interest in and capacity to pursue advanced and specialised learning opportunities in cyber security.

While Colombia has made substantial progress to improve internet connectivity and the use of information and communication technologies (ICT), a significant share of the population still lacks basic digital and technical skills. This hinders the digital transition and the ability to meet labour market demands, particularly in cyber security (OECD, 2021[2]). In Colombia 59% of all companies face challenges in IT and technology-related fields finding the talent they need (Manpower Group, 2022[3]).

The shortage of cyber security skills in Colombia likely stems from the fact that it is an emerging field. Education and training systems that provide cyber security programmes are still adapting to employers' requirements and to learners' ability to acquire these skills. Colombia faces several challenges and opportunities in this context. Firstly, it is vital to establish skill policy frameworks to create the right environment for the expansion of cyber security education and training. Increasing flexibility in provision, in particular within higher education institutions, can help to respond swiftly to changing skills needs in the sector and serve a diverse group of learners. Providers also need creative strategies to tackle teacher shortages in ICT. Secondly, the lack of basic digital skills and low English proficiency in the population is a common barrier to participation in cyber security learning opportunities. Moreover, women are hugely underrepresented in the ICT sector, and making the cyber security profession more appealing to women can help both promote equity and respond to employer needs.

Following this introduction, this chapter first provides a snapshot of cyber security education and training programmes in Colombia. This is followed by a discussion of efforts to develop a framework that allows the Colombian skills system to respond to labour market needs in the field of cyber security. The final section discusses strategies and policies in place to stimulate greater participation in these programmes, including initiatives aimed at enhancing digital literacy and facilitating access for underrepresented learners.

The information in this chapter is derived from interviews conducted with key stakeholders in the cyber security sector, including training providers and various government entities. The analysis also draws on desk research and analysis of data form multiple household surveys and administrative information.

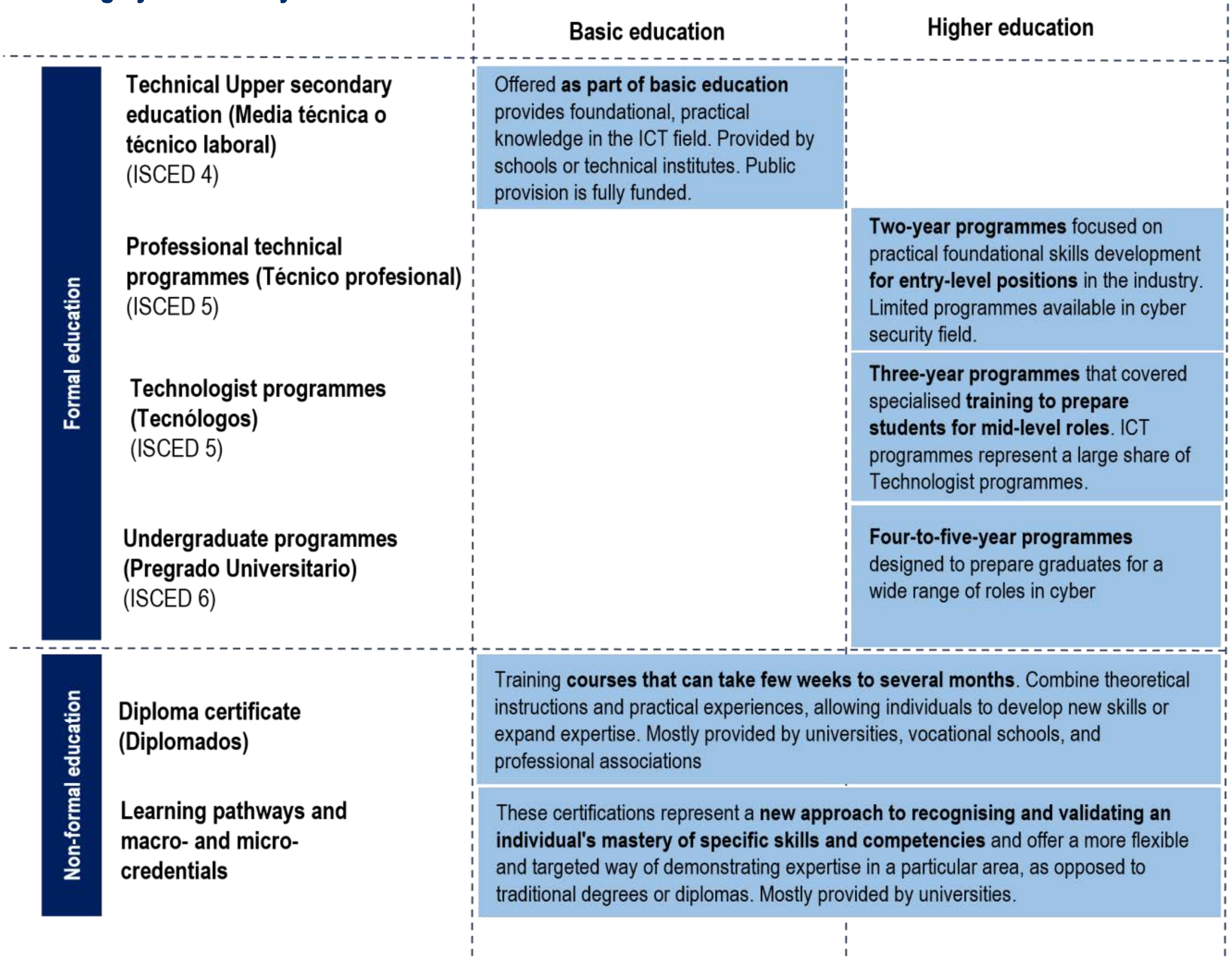
A glimpse into cyber security education and training programmes in Colombia

This section provides an overview of the education and training landscape in cyber security skills in Colombia. It first describes formal and non-formal education and training programmes that focus on cyber security, mostly within higher education. This is followed by a description of the profile of learners who pursue programmes in cyber security and an analysis of labour market outcomes associated with programmes in cyber security.

The provision of cyber security education and training in Colombia

Cyber security education and training aimed at developing skills for entry-level jobs include both formal and non-formal programmes[1] (see Figure 3.1). Formal education includes professional technical (two-year programme at ISCED Level 5), technologist (three-year programme, ISCED Level 5), and undergraduate programmes (four-to-five-year programme, ISCED Level 6) specific to this field, with the majority of cyber security training being offered at the graduate level (specialisation and master's degree, ISCED Level 7). This study focuses on qualifications below or at ISCED Level 6 (see Box 3.1). In addition to cyber security-specific programmes, some programmes in systems engineering and related fields include cyber security education and training as part of their curriculum and course content, or as areas of emphasis covering topics such as information security, information systems management, ethical hacking, network security, and information auditing. Articulation arrangements are also common within the system and software engineering programmes, facilitating the transition between higher education qualifications. These articulation arrangements are also offered with an emphasis on cyber security.

Figure 3.1. An overview of formal and non-formal education programmes that cover ICT field including cyber security in Colombia



		Basic education	Higher education
Formal education	**Technical Upper secondary education (Media técnica o técnico laboral)** (ISCED 4)	Offered **as part of basic education** provides foundational, practical knowledge in the ICT field. Provided by schools or technical institutes. Public provision is fully funded.	
	Professional technical programmes (Técnico profesional) (ISCED 5)		**Two-year programmes** focused on practical foundational skills development **for entry-level positions** in the industry. Limited programmes available in cyber security field.
	Technologist programmes (Tecnólogos) (ISCED 5)		**Three-year programmes** that covered specialised **training to prepare students for mid-level roles**. ICT programmes represent a large share of Technologist programmes.
	Undergraduate programmes (Pregrado Universitario) (ISCED 6)		**Four-to-five-year programmes** designed to prepare graduates for a wide range of roles in cyber
Non-formal education	**Diploma certificate (Diplomados)**	Training **courses that can take few weeks to several months**. Combine theoretical instructions and practical experiences, allowing individuals to develop new skills or expand expertise. Mostly provided by universities, vocational schools, and professional associations	
	Learning pathways and macro- and micro-credentials	These certifications represent a **new approach to recognising and validating an individual's mastery of specific skills and competencies** and offer a more flexible and targeted way of demonstrating expertise in a particular area, as opposed to traditional degrees or diplomas. Mostly provided by universities.	

Note: This figure does not include all forms of non-formal education provided in Colombia.
Source: OECD elaboration based on information from the Ministry of National Education and websites of some universities offering non-formal education such as Universidad de los Andes, Universidad EAN, Universidad Javeriana, and Universidad EAFIT.

Box 3.1. Defining the scope of cyber security education and training for this case study

In Colombia, cyber security education and training covers a wide range of topics and cater to various levels of knowledge and expertise – from cyber security awareness, aimed at educating the general public on identifying and avoiding cyber threats, to more advanced technical skills, such as intrusion detection software management or penetration testing, designed for a specialised workforce in cyber security occupations. These technical skills are typically imparted through structured training programmes led by vocational and higher education institutions, with dedicated trainers and experts.

This study focuses on education and training programmes for entry-level cyber security roles. Such positions typically do not require substantial work experience or advanced degrees in the field, and therefore the focus in this chapter is on formal professional technical (two-year programme, ISCED 5), technologist (three-year programme, ISCED 5), and undergraduate (four-to-five-year programme, ISCED 6) courses, alongside comparable non-formal education and training programmes like diploma certificates. These foundational qualifications are instrumental in broadening access to the profession, promoting diversity, and providing steppingstones towards more advanced education and training.

For its data analysis, this study employs the Colombian-adapted versions of the International Standard Classification of Education (ISCED), Fields of Education and Training (ISCED-F 2013) and the International Standard Industrial Classification (ISIC Rev 4) to identify the cyber security field of study and sector, respectively. As shown in Table 3.1, the ISCED-F 2013 category "Design and Management of Information Systems, Network and Database", henceforth termed "Information Systems and Services", encompasses the cyber security field. The most relevant cyber security sectors are "Computer Programming, Consultancy, and Related Activities" and "Information Services Activities", although cyber security jobs can be found across many different sectors. These categories help identify individuals who have participated in cyber security education and training programmes, depending on the data source.

Table 3.1. Identifying cyber security occupations and sectors in the Integrated Household Survey (*Gran Encuesta Integrada de Hogares*, GEIH) in Colombia

Based on the Colombian adaptation of ISCED field of study classification			Based on the Colombian adaptation of ISIC classification for sectors	
Broad field	**Specific field**	**Detailed field**	**Division**	**Group – Class**
06 Information and communication technologies	061 Information and communication technology	0611 Computer use	62 Computer programming, consultancy, and related activities	621 Computer programming activities
		0612 Design and management of information systems, network and database.		622 Computer consultancy and computer facilities management activities
		0613 Software application development and analysis	63 Information service activities	631 Data processing, hosting and related activities
		0619 ICTs not elsewhere classified		632 Other information service activities

Note: The cells highlighted are field of studies not considered as part of cyber security within ICT field.
Source: DANE (2018[4]), Clasificación internacional normalizada de la educación – campos de educación y formación adaptada para Colombia (CINE-F 2013 A.C.) (*Normalised International Classification of Education – fields of education and training adapted for Colombia)*; DANE (2021[5]), Clasificación Industrial Internacional Uniforme de todas las actividades económicas – Revisión 4 adaptada para Colombia. (*International Standard Industrial Classification of all economic activities – Revision 4 adapted for Colombia)*.

Non-formal education and training encompasses courses that may lead to certificates but do not yield a formal qualification. *Diplomados* or Diploma certificates represent the most prevalent type of certified non-formal, short training courses in this field, providing targeted instruction and practical experience. The recent surge in demand for specialised ICT skills such as cyber security, has led to a notable expansion in other forms of short courses, such as micro- and macro-credentials. These courses offer flexible and accessible learning opportunities, allowing individuals to acquire the necessary expertise quickly and efficiently. By focusing on specific skill sets and competencies, these courses help address immediate local skill demands and enable professionals to stay abreast of the latest industry developments.

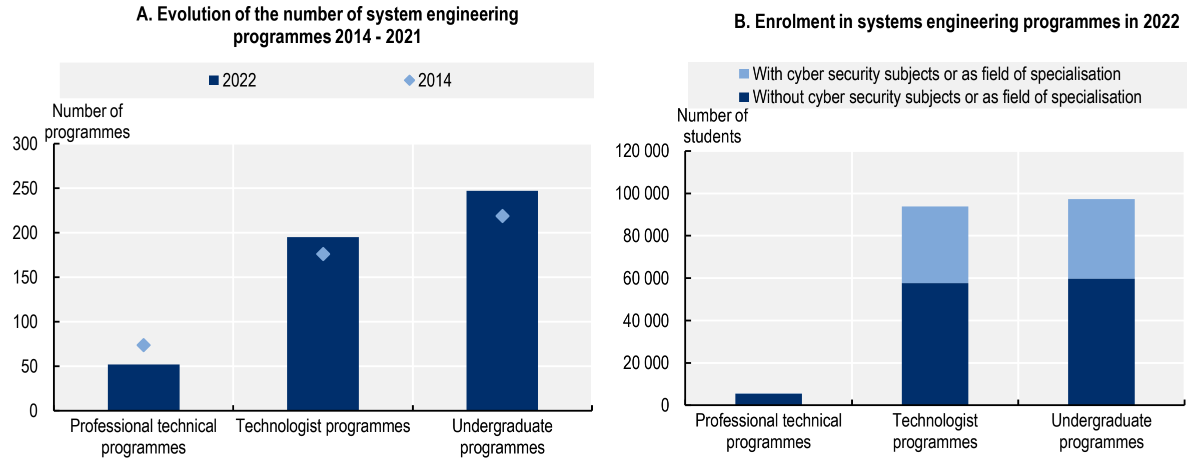
Formal and non-formal education in cyber security is delivered by various types of providers, each with distinct characteristics that cater to different learning needs and preferences. Higher education institutions, such as universities and technical institutes, offer formal programmes in fields related to cyber security, including systems engineering, computer science, and information technology. These institutions provide comprehensive, structured education and training, equipping students with a solid foundation in cyber security principles and practices. Universities and technical institutions can also provide non-formal education such as Diploma certificates. Private training centres, online learning platforms and industry-specific organisation offer only non-formal education programmes such as short courses, workshops and certifications in specialised cyber security sectors.

Formal education and training: The role of vocational and higher education

The provision of formal education programmes in cyber security in Colombia, specifically for entry-level jobs, covers various levels, ranging from professional technical and technologist programmes to undergraduate degrees. These programmes are designed to cater to the diverse educational and professional backgrounds of students, from those seeking entry-level skills to experienced professionals looking to enhance their expertise. In addition, technical upper secondary education mainly provides essential knowledge on ICT and aims to steer learners' interest towards further ICT training, but it does not cover cyber security subjects (see Box 3.2). Higher education includes vocational and undergraduate programmes. The former includes professional technical and technologist courses that focus on practice-oriented training, preparing students for careers in cyber security operations and management. Undergraduate programmes delve deeper into the theoretical foundations and advanced concepts of cyber security, emphasising research, innovation, and critical thinking. Depending on the level and type of programme, courses may be delivered full-time or part-time, while flexible schedules and blended learning options serve learners who cannot be fully dedicated to study or who are located in remote areas.

The offer of education programmes in this field has been growing in response to emerging demand. Colombian providers offered 494 formal programmes in systems, telematics, and related engineering fields in 2022 (hereinafter systems engineering programmes), including professional technical (52), technologist (195), and undergraduate programmes (247) (see Figure 3.2, Panel A). While the supply of technologist and undergraduate programmes in this field has increased by 12% compared to 2014, the number of more foundational technical programmes have dropped by 30%. The growth of technologist and undergraduate programmes may reflect higher demand for professionals with advanced skills in more technology-intense fields such as systems engineering (Ferreyra et al., 2017[6]). Also, the trend toward obtaining a higher education qualification may contribute to the decline in professional technical programmes in LATAM. Particularly in Colombia, the number of professional technical programme offerings across all fields has dropped by 39% in the last decade (MEN, 2023[7]). Students may increasingly pursue technologist and undergraduate degrees to improve their job prospects and earning potential (Ferreyra et al., 2017[6]). This trend can lead to a decrease in enrolment and offerings of more foundational professional technical programmes.

Figure 3.2. Provision of formal systems, telematics and related engineering programmes



Note: Information on subjects and specialisation areas in cyber security or information security was gathered from the websites of higher education institutions offering programmes in Systems Engineering, Telematics, and related disciplines.

Source: National Ministry for Education – National Information System of Higher Education (Sistema Nacional de Información de la Educación Superior – SNIES) – https://snies.mineducacion.gov.co/portal/.

Box 3.2. Technical upper-secondary education (Media técnica)

Technical upper-secondary education provides foundational technical knowledge in specific fields such ICT, preparing for entry-level jobs and advanced training at higher levels of education. It typically covers the final two years of basic education (i.e. students aged 15 to 16) and is delivered in vocational schools or technical institutes. Technical upper-secondary programmes offering ICT as area of specialisation introduce students to essential concepts and principles of ICT, developing theoretical knowledge and practical skills, drawing on up-to-date scientific and technical knowledge. Programmes also aim to foster student interest in the field, establishing a strong foundation for more advanced training in ICT areas such as cyber security.

Public institutions, predominantly National Learning Service (Servicio Nacional de Aprendizaje, SENA), lead the provision of technical upper secondary programmes, leveraging partnerships with local governments, city councils, and the business sector. For example, since 2015, the Medellín city council has built ties with various technical schools, like SENA and ETDH Microempresas de Colombia,[2] benefiting roughly 19 000 students across 189 institutions in 2019 with advanced ICT training (Medellin's Secretary of Education, 2022[8]). Similarly, Bogotá's city council has fostered educational continuity through projects like 'Strengthening the Skills of District Youth to Face the Challenges of the 21st Century,' which smooths the transition of students into ICT-specialised education (Alcaldía Mayor de Bogotá, 2021[9]).

The provision of cyber security programmes in formal education is relatively small but has been growing. While in 2014 no programmes existed in this field, by 2022 four cyber security programmes were available: one professional technical (in Information Security Services), three technologists (in Computer network and information security, in Computer Network Security Management and in Network and information security), and one undergraduate programme (Engineering in information security). In addition, 58% of systems engineering programmes include cyber security topics as subjects or as an area of emphasis.

Participation in education and training programmes in cyber security or related fields is limited. According to the National Information System of Higher Education (SNIES), in 2022, only 15% of students in higher education were enrolled in systems engineering programmes, and this proportion has fallen since 2016. Most learners who study systems engineering programmes cover cyber security topics (see Figure 3.2, Panel B). In 2022, two out of every five students in systems engineering technologist and undergraduate were enrolled in programmes that included cyber security subjects or offered cyber security as a field of specialisation. According to consulted stakeholders, the importance of cyber security within technologist and undergraduate programmes may be due to the complexity and prerequisites of the field, as well as the growing demand for professionals with advanced skills in cyber security. Conversely, only 4% of students of professional technical programmes in the field of systems engineering enrolled in a programme that covers cyber security subjects.

Professional technical and technologist programmes

In Colombia, ICT programmes at short-cycle tertiary level (ISCED Level 5) include two types of programmes: professional technical programmes and technologist programmes, with the latter providing more advanced knowledge and skills. These programmes are similar to associate degrees in the United States, higher technical qualifications in the United Kingdom and *Brevet de Technicien Supérieur* (BTS) programmes in France. Both professional technical and technologist programmes prepare for entry into the labour market, while allowing for progression to higher levels of education. Delivered by vocational and technical institutions, they target various ICT disciplines such as programming, network administration, and systems management. Both professional technical and technologist programmes are designed through collaboration between employers and educational providers, ensuring that the course content meets industry demands. The National Learning Service (SENA), the largest public professional technical and technologist provider, engages with employers through sectoral roundtables to design and update programmes and curricula. Three out of 84 sectoral roundtables concentrate on the ICT sector, covering areas like digital and information security (SENA, 2023[10]). This approach ensures alignment between educational programmes and the evolving needs of the ICT industry.

Professional technical programmes emphasise foundational skills in ICT. Programmes take two years to complete and usually involve a work-based learning component. They include areas such as hardware and software technical support, as well as software programming. In 2022, only one programme was offered in the field of cyber security (see Table 3.2, first row) with 45 students enrolled. This programme provides foundational knowledge and skills in cyber security such as running vulnerability threat and risk tests and implementing cyber security protocols. Most professional technical programmes focus on broader ICT education, with cyber security addressed as one component within the curriculum. For example, some programmes have modules or courses related to cyber security, such as network and risk management, and incident response. According to SNIES, 11% of professional technical programmes in the field of system engineering include cyber security subjects (6 programmes in total) such as ‘support of information system security’ and ‘introduction to information security’. This approach ensures that students gain a comprehensive understanding of ICT concepts, while developing some specialised knowledge and skills in cyber security. The curriculum is structured to incorporate real-world scenarios and practical exercises, encouraging students to apply their learning to address current and emerging cyber security challenges.

Table 3.2. A sample of cyber security professional technical programmes in Colombia, 2022

	Programme	Duration	Description	Provider and location
Professional technical programmes in cyber security	Professional technician in information security services	4 semesters	A professional technician in computer security services is able to monitor and provide support and solutions in computer security. In this programme, students learn how to run vulnerability threat and risk test following technical policies and protocols available in the cyber security field.	Fundación Polítécnico Minuto de Dios, in Bogota
Professional technical programmes including cyber security subjects or as area of emphasis	Professional technician in software and hardware support	4 semesters	This programme equips students with foundational technical skills to implement, operate, and maintain systems and applications using tools, enabling them to provide support in the use of computer systems. This programme include training on information security and support of information systems.	Instituto superior de educación social (ISES)

Source: MEN (2023[7]), Sistema Nacional de Información de la Educación Superior – SNIES *(National Higher Education Information System)*, https://snies.mineducacion.gov.co/portal/; Fundación polítécnico Minuto de Dios (2023[11]), Técnico profesional en servicios de seguridad informática *(Professional technician in information security services)*, https://tecmd.edu.co/programas_titulados/tecnico-profesional-en-servicios-de-seguridad-informatica/; Instituto superior de educación social (ISES) (2023[12]), Técnico profesional en soporte de hardware y software *(Professional technician in software and hardware Support)*, https://www.ises.edu.co/soporte-de-hardware-software.

Technologist programmes in cyber security provide a more advanced level of education than technical programmes, preparing students for mid-level roles in the industry. These programmes typically involve both theoretical instruction and practical applications, with emphasis on problem-solving and critical-thinking skills (MEN, 2023[13]). The durations of technologist programmes in cyber security are generally between two and three years. Programmes cover a wide range of topics, including network security, ethical hacking, digital forensics, risk management, security operations, and incident response. Students are also exposed to emerging technologies and trends in the field, such as cloud security, Internet of Things (IoT) security, and artificial intelligence applications in cyber security. Three technologist programmes focus specifically on cyber security: 'Computer network and information security', 'Computer network security management' and 'network and information security' (see Table 3.3). In addition, students can select among the 63 programmes in the field of system engineering which include cyber security as part of the programme structure or as an area of emphasis. For instance, the technologist school 'Institución Universitaria Salazar Herrera' in Medellin offers a programme in 'Technologist in systems', with information security as area of specialisation. This area includes three subjects: 'ethical hacking', 'network security' and 'security testing'

Table 3.3. A sample of cyber security technologist programmes in Colombia, 2022

	Programme	Duration	Description	Provider and location
Technologist programme in cyber security	Technologist in computer network and information security.	6 semesters	This programme offers students theoretical and practical foundation to implement security controls, configure devices securely, manage vulnerabilities an detect network security incidents	Corporación Universitaria Minuto de Dios (Uniminuto), in Bogota
	Technologist in computer network security management.	6 semesters	This programme offers students the foundations to provide technological support for network-based services and resources, as well as carry out vulnerability management, reporting, monitoring, and detection of security incidents and consolidate network performance metrics.	Corporación Universitaria Minuto de Dios (Uniminuto), in Bogota.
	Technologist in Network and information security.	6 semesters	Students enrolled in this programme are able to set up, give support and ensure secured connectivity in organisations. This programme also provides foundations for risk management for highly technological environments and big data infrastructure.	Institución Universitaria Escolme, in Antioquia
Technologist programmes including cyber security subjects or as area of emphasis	Technologist in Systems with emphasis on information security	6 semesters	Students in this programme engage in developing and implementing computer applications for desktop and mobile devices, as well as designing and managing computer networks for various organisations. This programme offers students security information as specialisation pathway.	Institución Universitaria Salazar y Herrera
	Technologist in Software development.	6 semesters	The Technologist in Software Development programme provides students with essential skills for the software industry. Focusing on efficient processes and social, technical, economic, and environmental responsibility, the curriculum covers four key areas: operational design, information system development, software testing, and database maintenance and support.	Institución Universitaria Pascual Restrepo
	Technologist in Development of informatic systems.	6 semesters	A technologist from this programme will be capable of efficiently implementing a software product and performing its respective maintenance. This programme includes several subjects related to computer security, such as information technology security, information systems planning, and server administration.	Unidades tecnológicas de Santander

Source: MEN (2023[7]), Sistema Nacional de Información de la Educación Superior – SNIES *(National Higher Education Information System)*, https://snies.mineducacion.gov.co/portal/; Fundación polítécnico Minuto de Dios (2023[14]), Técnico profesional en servicios de seguridad informática *(Professional technician in information security services)*, https://tecmd.edu.co/programas_titulados/tecnico-profesional-en-servicios-de-seguridad-informatica/; (2023[15]), Tecnologías en sistemas *(Technologist in systems)*, https://www.iush.edu.co/es/Universidad/pregrados/escuela-de-ingenierias/tecnologia-sistemas; Institución Universitaria Pascual Restrepo (2023[16]) Tecnología en desarrollo de software *(Technologist in Software development)*, https://pascualbravo.edu.co/facultades/facultad-de-ingenieria/programmeas/tecnologia-en-desarrollo-de-software/; Unidades tecnológicas de Santander (2023[17]), Tecnologia en Desarrollo de Sistemas informáticos *(Tecnologist in development of informatic systems)*, https://www.uts.edu.co/sitio/tecnologia-en-desarrollo-de-sistemas-informaticos/#1562800770722-cfdcde65-4afc; Institución Universitaria Escolme (2023[18]), Tecnologo en redes y seguridad informática *(Technologist in Network and information security)*, www.escolme.edu.co.

Undergraduate programmes

Undergraduate programmes (ISCED Level 6) in Colombia take four to five years to complete. ICT programmes provide students with a solid expertise in various aspects of ICT, while also offering the opportunity to delve deeper into cyber security-related subjects through specialised coursework, projects, or internships. The curriculum typically covers essential topics such as cryptography, network security, ethical hacking, software security, and information assurance, while also incorporating cross-cutting topics and technologies like cloud security, IoT security, and artificial intelligence in cyber security. Only one undergraduate programme is available in cyber security. However, most undergraduate programmes in system engineering cover cyber security topics as part of the curriculum or area of emphasis (58% in 2022) (see Figure 3.2, Panel B).

Table 3.4 describes a cyber security programme and a system engineering programme with an emphasis in cyber security. The former provides students with a comprehensive understanding of cyber security issues from the beginning. Further in the training, it provides specialised knowledge on hacking techniques, forensics, databases and infrastructure security. System engineering programmes with cyber security content also include specialised training in cyber security-specific topics such as software security and infrastructure security, however, most of these subjects are not compulsory. Both programmes combine theoretical foundations with practical applications relevant to a wide range of cyber security roles, from security analysts and consultants to network administrators and digital forensic specialists, including cyber security research (see Chapter 2).

Table 3.4. A sample of cyber security undergraduate programmes in Colombia, 2022

Programme	Duration	Description	Provider and location
Information security engineering	9 semesters	This programme offers knowledge and skills to secure, audit, and protect information. Students completing this programme have a critical and creative vision to mitigate and manage the risk according to the current communication needs of public, private and governmental institutions. Students are prepared in state-of-the-art technologies for certification in cyber security tools and standards from world-class companies such as Cisco, Fortinet, ISO 27000, Microsoft and Linux	Universidad de Manizales, in Caldas
System engineering	8 semesters	The focus on advanced software development and digital security covers two areas: infrastructure, which targets secure solutions for lower computer system layers, and development, which aims to create complex applications for upper layers.	Pontificia Universidad Javeriana, in Bogotá

Source: MEN (2023[7]), National Higher Education Information System (Sistema Nacional de Información de la Educación Superior – SNIES); Universidad Javeriana (2023[19]), Ingenieria de sistemas *(Systems engineering)*, https://www.javeriana.edu.co/carrera-ingenieria-de-sistemas; Universidad de Manizales (2023[20]), Ingenieria en seguridad de la información *(Information security engineering),* https://umanizales.edu.co/Programmea/ingenieria-en-seguridad-de-la-informacion/.

Most undergraduate programmes in systems engineering provide a range of degree pathways and cater to diverse student interests and career goals. One popular option involves participating in industry internships, apprenticeships or work placements during the final year of study (MEN, 2015[21]). These hands-on experiences, which typically last between one semester and a year, enable students to gain valuable insights and practical skills within the sector. Alternatively, students may opt to pursue postgraduate studies early by enrolling in master's level courses in information security or other related fields during their final year of undergraduate education. This approach allows for a smoother and faster transition into advanced studies.

Articulation arrangements between different levels

In higher education, students can also enrol in articulated programmes in ICT fields, designed to facilitate transitions between levels. The term "propaedeutic cycle" is commonly used in Colombia to refer to articulation arrangements and it is particularly common in systems and software engineering degrees (see Box 3.3). Articulation arrangements play a crucial role in smoothing the transition from general ICT technical programmes to technologists and undergraduate programmes such as software engineering with emphasis in cyber security. The framework is flexible, so students can choose the intensity and level of specialisation. This approach is designed to prepare students for more specialised studies in their chosen field, building on the solid foundation in core ICT concepts and principles they already acquired (MEN, 2017[22]).

Table 3.5 shows some of the universities that offer this propaedeutic cycle in system engineering or software engineering with emphasis on cyber security. For instance, Colombian Industrial Technologist school (*Corporación Tecnológica Industrial Colombiana* – TEINCO) offers a two-years technical programme in information system which equip students with skills to manage databases, websites and information systems and implement protocols for software development. After finishing, students can enroll to obtain a technologist degree in software development by adding one more year of specialised studies, and taking more field specific subjects such as system information design and software and system analysis. If students are interested in obtaining an undergraduate degree in systems engineering with emphasis in cyber security, they only require an additional year and a half of advanced courses such as software development, system auditing, and ethical hacking.

Table 3.5. Programmes with propaedeutic cycle with system engineering or software engineering with focus on cyber security

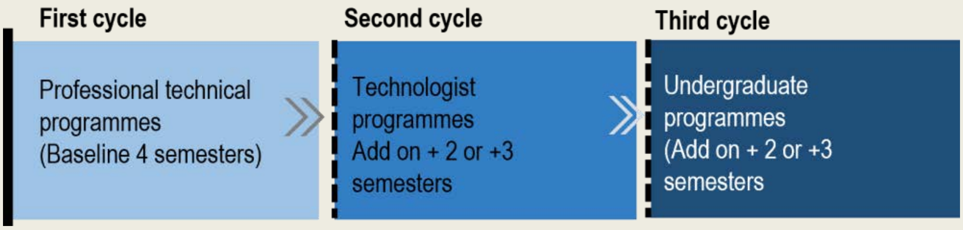
Programme	Level of education	Duration	Description	Provider and location
Professional technician in Information system (Baseline programme)	Technical programme (ISCED 5)	4 semesters	This programme equips students with the foundational technical skills to develop information systems and websites, manage databases, and implement protocols for software development.	Corporación Tecnológica Industrial Colombiana – TEINCO
Software development technology	Technologist programme (ISCED 5)	+ 2 semesters	In the additional two semesters, the programme provides the technical knowledge on system information design, cyber security, software engineering and system analysis.	
System engineering	Undergraduate programmes (ISCED 6)	+3 semesters	In the last three semesters, the programme imparts more advanced training on system auditing, ethical hacking, software engineering, and informatic legislation.	
Professional technician in software programming (Baseline programme)	Technical programme (ISCED 5)	4 semesters	This programme equips students with skills to identify organisational needs, automate data processing, implement information management policies, develop software applications, and provide hardware and software technical assistance.	Corporación Institución de Administración y Finanzas
Software development technology	Technologist programme (ISCED 5)	+ 3 semesters	In the additional three years, the programme covers data processing automation, software development engineering, quality, and advanced networking and database management skills.	
Software engineering	Undergraduate programmes (ISCED 6)	+3 semesters	In the final three years, students learn advanced software engineering, artificial intelligence, software auditing, information security, and secure systems architecture.	

Note: The starting programme is highlighted in grey.
Source: MEN (2023[7]), National Higher Education Information System (Sistema Nacional de Información de la Educación Superior – SNIES); Corporación Tecnológica Industrial Colombiana (TEINCO) – https://teinco.edu.co/; CIAF Institución de Educación Superior – https://www.ciaf.edu.co/landing/vistas/IngenieriadeSoftware.html.

Box 3.3. Propaedeutic cycle in Colombia: Technical, technologist and undergraduate programmes articulation

Higher undergraduate education in Colombia is organised into three flexible, sequential, and complementary stages through propaedeutic cycles, which is a preliminary stage in an education programme that equips students with the foundational knowledge and skills needed for advanced study in a specific subject area. Students can start with a professional technical programme (2 or 3 years), progress to a technologist programme (+1 year), and finally attain a university professional level (+1 or +2 years) (See Figure 3.3). Propaedeutic cycles allow students to opt for a professional technical or technologist career, earning a degree certifying their specific competencies. Graduates can then proceed to the next cycle, obtaining a corresponding degree. Each cycle also offers opportunities for specialisation.

Figure 3.3. Structure of a propaedeutic cycle


First cycle
Professional technical programmes (Baseline 4 semesters)
Second cycle
Technologist programmes Add on + 2 or +3 semesters
Third cycle
Undergraduate programmes (Add on + 2 or +3 semesters

Source: OECD elaboration based on information from Ministry of National Education, https://www.mineducacion.gov.co/portal/Educacion-superior/Informacion-Destacada/196476: Formacion-por-ciclos-propedeuticos.

As stated in Law 749 of 2002, the first cycle encompasses professional technical training, focusing on tasks related to independent technical activities. The second cycle pertains to technologist training, developing "responsibilities of conception, direction, and management." The third cycle constitutes the professional level, enabling "autonomous practice of high-level professional activities and mastery of scientific and technical knowledge." Every cycle serves a unique educational purpose, professional profile, and performance field. The aim is to create a coherent, interconnected chain of cycles, forming a multilevel training process with increasingly complex and broader competencies (Congreso de Colombia, 2002[23]).

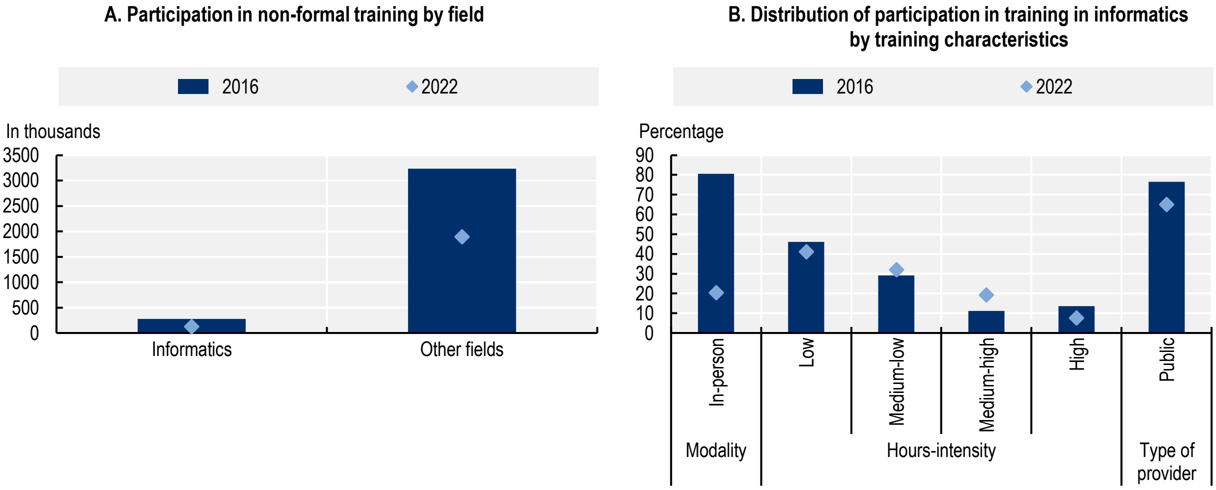
Source: Ministry of National Education, https://www.mineducacion.gov.co/portal/Educacion-superior/Informacion-Destacada/196476: Formacion-por-ciclos-propedeuticos.

Non-formal training: Continuing education and job training programmes

Non-formal education and training in cyber security in Colombia takes many forms, addressing various topics within the field and catering to a wide range of learners. These programmes, which include short-term courses, online learning, and specialised training offered by higher education institutions, industry experts, and private organisations, provide flexible learning opportunities for individuals seeking to develop or enhance their cyber security skills. Within this diverse landscape, this section focuses on the most relevant and innovative initiatives, such as Diplomados or Diploma certificates and the novel offer led by higher education institutions such as micro- and macro-credentials and non-formal learning pathways. These training programmes aim to respond to labour market needs and encourage broader and diverse participation in training.

In Colombia, participation in non-formal education has dropped in all fields of study including informatics and engineering (which are related to cyber security). Panel A of Figure 3.4 shows that around 2.1 million individuals participated in non-formal training in 2022, 42% less than in 2016. The COVID-19 pandemic largely explains this drastic decline in participation in non-formal education. Compared to 2021, after the peak of the COVID-19 pandemic, the number of participants in non-formal training increased by 18% (DANE, 2022[24]). The drop in enrolment is more pronounced in fields different from informatics and engineering which reflects that the demand of ICT skills training remains strong. Also, with the rise of online learning platforms and Massive Open Online Courses (MOOCs), individuals may prefer accessing training and educational content online rather than attending non-formal training person, and such remote options are more often available in the ICT field. In 2022, 80% of non-formal learners enrolled in informatics and engineering took their training online – almost four times more than in 2016 (see Figure 3.4, Panel B). Most of the learners of informatics and engineering non-formal training are enrolled in short or low- and medium-low-intensity courses (less than 100 hours of training) (73%) and in those mainly provided by public institutions (65%).

Figure 3.4. Participation non-formal training in informatics



Note: Informatics includes cyber security training. Computations are based on the GEIH module of 'training for employment' which covers everyone aged 15 and above. The intensity of the training is measured in hours: Low intensity refers to less than 40 hours of training; medium-low intensity to between 41 and 100 hours; medium-high to between 101 and 600 hours; and high to between 601 and 1 800 hours. Number of participants includes individuals who report participating in non-formal training at the time of the survey and those who had participated within the last 24 months.
Source: OECD calculations using the Integrated Household Survey 2022 (*Gran Encuesta Integrada de Hogares* – GEIH).

Informatics is one of the fields learners are most engaged in after 'business and administration', 'health and social services' and 'security services' (DANE, 2022[25]). Around 175 thousand people participated in training in informatics in 2022, which reflects the government's effort in expanding access to ICT training by funding formal and non-formal programmes. Strategies such as 'A ticket for the future' (*Un tiquete para el futuro*) and 'Digital skills in cyber security' are among the initiatives implemented in the last five years (MinTIC, 2022[26]; 2022[27]), as discussed later in this chapter.

Diploma certificates (*Diplomados*)

Diploma certificates are short, intensive courses that provide specialised education and training in a specific subject or field, such as cyber security. This type of training serves a diversity of students, including working professionals and those seeking a career change. Diploma certificates are not regulated by the municipal secretary of education or MEN (Ambito Jurídico, 2022[28]), however, they are considered the most common non-formal training available and in high and increasing demand by potential learners (El Colombiano, 2021[29]). Ranging in duration between 40 and 120 hours, Diploma certificates combine theoretical instruction and practice-oriented learning experiences (MEN, 2020[30]). They serve as a flexible and accessible form of non-formal education, allowing individuals to expand their expertise and keep up with industry trends. Diploma certificates typically take between 3 to 12 months to complete and involve practical training, case studies, and group discussions. Their costs vary substantially, ranging between COP 600 000 (Colombian Pesos) and COP 4 500 000 (approximately EUR 120 and EUR 915),[3] depending on the length and course content. These courses are highly specialised and can be taken in-person or online. Their schedule is flexible, and courses may be offered on evenings and/or weekends, to allow students to balance their studies with other commitments.

The content of diploma certificates in cyber security can vary by level of difficulty and specialisation (see Table 3.6). General diploma certificates equip students with foundational technical knowledge in cyber security and computer security management. These courses also aim to raise awareness about information security issues and cyberattacks. For instance, Javeriana University offers an online diploma certificate that introduces cyber security operations, covering the essential knowledge for understanding cyber security fundamentals. Other diploma certificates address more advanced and complex topics, such as Universidad del Bosque's diploma certificate focused on Ethical Hacking. This programme enables students to develop knowledge about the technical, strategic, and legal aspects of computer security. Some diploma certificates go hand in hand with competency certifications or industry-required standards. For example, Universidad Piloto de Colombia's computer security diploma certificates includes an Internal Auditor course and certification in ISO 27001, which is deemed highly relevant in the sector.

Table 3.6. A sample of Diploma certificates in cyber security

Programme	Duration	Modality	Description	Provider
Diploma certificate in Introduction of cyber security operations	51 hours	Virtual / Online	This course provides comprehensive training in cyber threats and information security risk for students pursuing a cyber security career, enabling them to identify vulnerabilities and respond effectively.	Pontificia Universidad Javeriana, Bogotá
Diploma certificate in cyber security	120 hours	Virtual / Online Synchronous	This course equips students with skills to create and implement policies ensuring an organisation's computer resources' confidentiality, integrity, and availability. The curriculum covers topics such as cyber security, network security, software development security, penetration testing, and cyber security management.	Universidad del Norte, Barranquilla
Diploma certificate in computer security	100 hours	In person	The computer security diploma certificate equips students with tools to counter threats and implement information protection schemes aligned with ISO 27001 standards. The 65% practical programme includes labs in cryptography, vulnerability analysis, ethical hacking, digital forensics, and workshops on risk management, business continuity, and auditing.	Universidad Piloto de Colombia, Bogotá
Diploma certificate in Ethical Hacking	100 hours	Virtual / Online	This diploma certificate aims to tackle challenges related to information security and data protection by comprehensively addressing strategic, technical, and legal aspects, all while adhering to industry regulations and employing best practices	Universidad del Bosque, Bogotá

Source: Universidad del Norte – https://www.uninorte.edu.co/web/educacion-continuada/diplomado-en-ciberseguridad; Universidad Piloto de Colombia, https://www.unipiloto.edu.co/diplomado-en-seguridad-informatica/; Tech school of information technology https://www.techtitute.com/co/informatica/diplomado/seguridad-informatica; Pontificia Universidad Javeriana, https://javerianacyberpro.com/ciber-academia/introduccion-a-la-ciberseguridad/.

Typically, diploma certificates are offered by higher education institutions, professional associations, and private organisations. Some educational institutions form partnerships with private sector companies or specialised international providers. One example is the collaboration between the Pontificia Universidad Javeriana and CyberPro Global, a leading international provider of cyber security education and training. Together, they have established the Javeriana CyberPro Centre, which aims to identify training needs and offer comprehensive cyber security education and support (see Box 3.4). Similarly, SENA developed the ‘Technological centre of excellence and simulation in cyber security’ jointly with MNEMO (an IT and cyber security services company) to deliver diploma certificates in information security and courses related to the field.

Box 3.4. Partnerships to provide Diploma certificates in cyber security

Javeriana CyberPro Centre

The Pontificia Universidad Javeriana and CyberPro Global have partnered to create Colombia’s first cyber security Centre, the Javeriana CyberPro Center. Offering an innovative approach, the centre combines different educational methods, practical challenges, and cyber services. It provides diploma certificate courses focused on cutting-edge technologies for cyber security and information security professionals.

- Cyber-Fundamentals: Students explore crucial aspects of the cyber landscape, gaining knowledge for a cyber security career. The course covers importance, tools, and concepts through hands-on exercises in specialised environments for an engaging learning experience.
- CISO: Designed for managers with at least three years of experience in IT, departments, divisions, or security, this programme enhances participants’ cyber security management expertise and helps them achieve international certification. The course focuses on understanding planning and maintenance processes for integrated security management systems, equipping students with the tools to lead technology teams effectively.
- Cyber-awareness: This programme cultivates a strong cyberculture within organisations by educating employees and creating a “human firewall.” It emphasises sharing best practices among management, employees, and stakeholders to prevent or mitigate security breaches. Participants gain the knowledge and tools to understand risk and implement suitable policies.

The Javeriana CyberPro Center also provides tailored training programmes for companies with distinct cyber security needs. These organisations benefit from initial consultation and a customised proposal addressing their requirements, resources, schedule constraints, and other considerations.

Technological Center of Excellence and Simulation in Cyber security (SENA-MNEMO).

The National Learning Service (Servicio Nacional de Aprendizaje – SENA, a public VET institution) together with MNEMO, an IT and cyber security services company, founded the Center of Technological Excellence (Centro de Excelencia – CEDEX) to deliver comprehensive training for instructors and learners in the field of cyber security. Through this collaboration, they provide various educational opportunities, including trainings, diploma certificates, bootcamps, and international certifications. The centre also features a specialised laboratory for immersive classes, allowing students to practice in real-world company environments. Since the centre’s inception, approximately 23 000 students in the ICT sector have benefited from its offerings.

Source: CYBERPRO Center (2023[31]), Javeriana Cyberpro centre, https://javerianacyberpro.com/; MNEMO (MNEMO, 2022[32]) – SENA y MNEMO inauguran en Colombia el primer centro tecnológico de excelencia y simulación en ciberseguridad de América Latina (*SENA and MNEMO launch Colombia’s first cybersecurity technology centre of excellence and simulation in Latin America*), https://www.mnemo.com/sena-mnemo-ciberseguridad/.

Other types of short courses, non-traditional learning pathways and online training

Diploma certificates are only one form of non-formal education and training programmes. The non-formal training sector is hugely diverse, with different types of training modalities and covering a variety of sectors. Short courses, like diploma certificates and many other non-formal training activities, have become some of the most common types of non-formal training among learners interested in the field of informatics and engineering (see Figure 3.4, Panel B). These courses usually last a few weeks or months and are often available online and cover a wide range of topics, from foundational knowledge in cyber security, to more specialised topics depending on the course's focus.

In recent years, due to the high demand for ICT skills, the provision of short-term courses in Colombia has become more structured, offering them as part of learning pathways or building blocks for developing more advanced and specialised skills, such as in cyber security. Micro- and macro-credentials[4] are examples of these initiatives, validating and certifying the mastery of specific skills or competencies as part of a learning path in a specific field. In some cases, micro- and macro-credentials can be recognised as part of academic credits (i.e. measure of the value or weight assigned to a particular course or module) within a formal programme. For example, Universidad EAN provides training pathways in ICT skills within the cyber security sector. Paths such as 'software development,' 'information management and databases,' and 'network and communication management' enable students to acquire micro and macro-credentials, validating their knowledge and facilitating access to job opportunities or the recognition of subjects that are part of a formal educational programmes. Some of these short courses are provided online and through e-learning platforms (see Box 3.5).

Box 3.5. Online courses in digital skills available in Spanish: Insights from e-learning platforms

The top e-learning platforms in Latin America, including Coursera, EdX, LinkedIn Learning, and Tutellus (Edapp, 2022[33]), offer around 40 000 digital skills and computer science courses, with 24% of the total online course offerings being in the digital field (see Table 3.7). Cyber security course availability is limited, but LinkedIn Learning provides the most extensive selection, with 530 Spanish-language courses as of April 2022. Courses cater to different levels of expertise, budgets, and time commitments, ranging from beginner topics to advanced certification programmes. Learners with no experience in the field can enrol in courses such as 'Information Security Principles and Regulations (*Principios y regulaciones de seguridad de la información*)'. For learners with more experience, there are options such as 'Vulnerability and penetration test (*Vulnerabilidades y pruebas de penetración*)' or 'Cyber security for Tech Professionals (*Ciberseguridad para profesionales de ICT*)'. These platforms also update their course offerings regularly to keep up with industry trends and emerging technologies.

Table 3.7. Online short courses offered in Spanish on a selected of e-learning platforms

Online training provider / Platform	Total number of training courses (approx.) *	Total number of courses offered in digital skills and computer sciences	% Out of the total number of courses offered	Total number of courses offered in cyber security	% Out of the total number of courses offered in computer sciences
Coursera	4 500 +	978	22	15	2
EdX	700 +	106	15	11	10
LinkedIn Learning	16 000+	4 133	26	530	13
Udemy	17 000+	2 748	2	301	11
Tutellus	NA	1 240		11	
Total	38 000+	9 205	24	868	9

Note: The numbers for digital and computer science and cyber security were retrieved from each platform course finder. The filters available by default were used for the number of digital and computer science courses. For the number of cyber security courses, "cyber security" word combinations were used in each platform's search engine after filtering by digital and computer science fields. Only the courses offered in Spanish were taken into account.
Source: Information collected online directly from providers' platforms on April, 2022. The total number of training courses is taken from the e-learning platform websites.

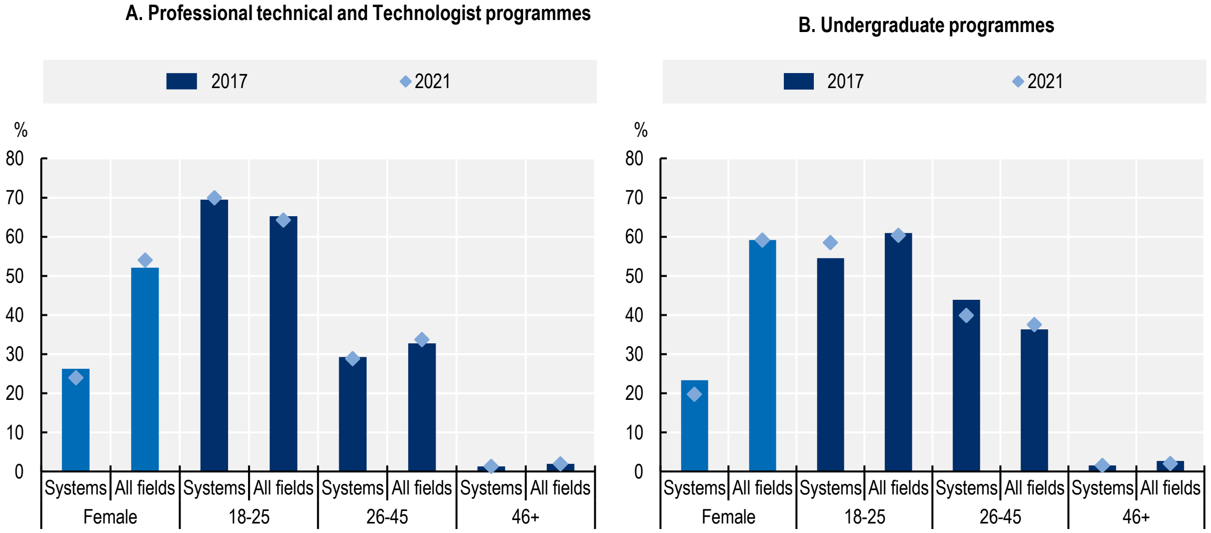
The profiles of cyber security learners

Diversity among cyber security learners

Cyber security education and training programmes are accessible to learners of all ages. However, in formal education, a significant portion of learners in technical professional, technologist and undergraduate programmes in systems engineering are from the younger cohorts (see Figure 3.5). In 2022, the majority of students nearing completion of technical, technologist programme, or higher education programmes in systems engineering were between 18-25 years old (70% and 59%, respectively), and this share has increased compared to 2017. Conversely, participation of older learners (46+) in cyber security education and training is limited. This is consistent with international research that finds that teens and young adults who faces rapid adoption of mobile internet and faster appropriation of technology, have more changes to engage with STEM education and aspired to work in STEM jobs (Godec, Archer and Dawson, 2021[34]).

Figure 3.5. Enrolment in formal education programmes in systems engineering field, by sociodemographic characteristics

Share of students close to completion of formal education programmes



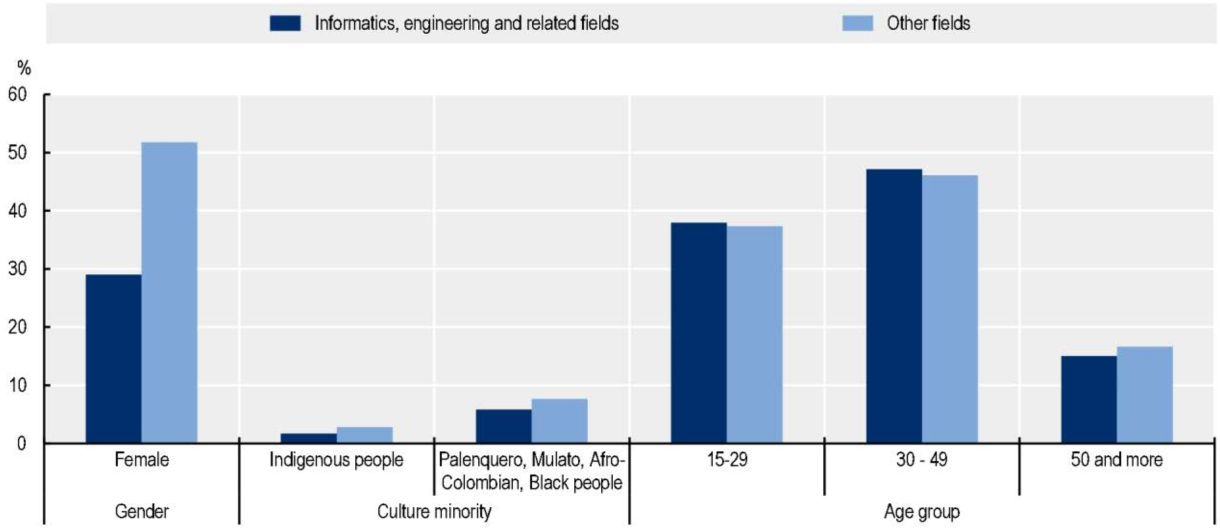
Note: Label on the horizontal axis refers to Systems engineering and telematics and related fields. Saber Pro is a learning assessment applied to students enrolled in professional technical and technologist programme (ISCED 5) and undergraduate programme (ISCED 6) that are about to complete their studies. The exam is mandatory.
Source: OECD calculations using Saber Pro learning assessment from the Colombian Institute for the Evaluation of Education (Instituto Colombiano para la Evaluacón de la Educación – ICFES) – https://www2.icfes.gov.co/data-icfes.

In non-formal training, learners from different age groups engage with training in cyber security related fields. Figure 3.6 shows that in the participation rate in informatics and engineering training is higher among 30-49 year-olds than any other age group (47%). Also, young people are more likely to enroll in cyber security related field training than those aged 50 or more (38% vs. 15% respectively).

Similarly to other countries, ICT in Colombia is a male-dominated field. In 2022, around one-fifth of students about to complete their technical and technologist programme (24%) and undergraduate programmes (20%) were women, and this ratio has slightly decreased in the last five years (see Figure 3.6). In non-formal training, women are also underrepresented: only 29% of learners in informatics and engineering are females, which is noticeably less than the proportion of women studying in other fields (52%). The Colombian Government has made progress in providing information regarding labour market outcomes especially in the STEM field, such as the Proyecta-T programme (MEN, 2015[35]), and the labour opportunities available for women in the sector, but policies oriented to guide students to use the information available and support their career decision making process (Bonilla-Mejía, Bottan and Ham, 2019[36]), especially among women, may remain insufficient. Colombia has experienced high levels of economic inequality, which can disproportionately affect women and limit their access to educational resources, including career guidance. Also, lack of female role models in the ICT field make young women less likely to pursue an ICT career path.

Figure 3.6. Participation in non-formal training in informatics, by socio-demographic characteristics in 2022

Percentage



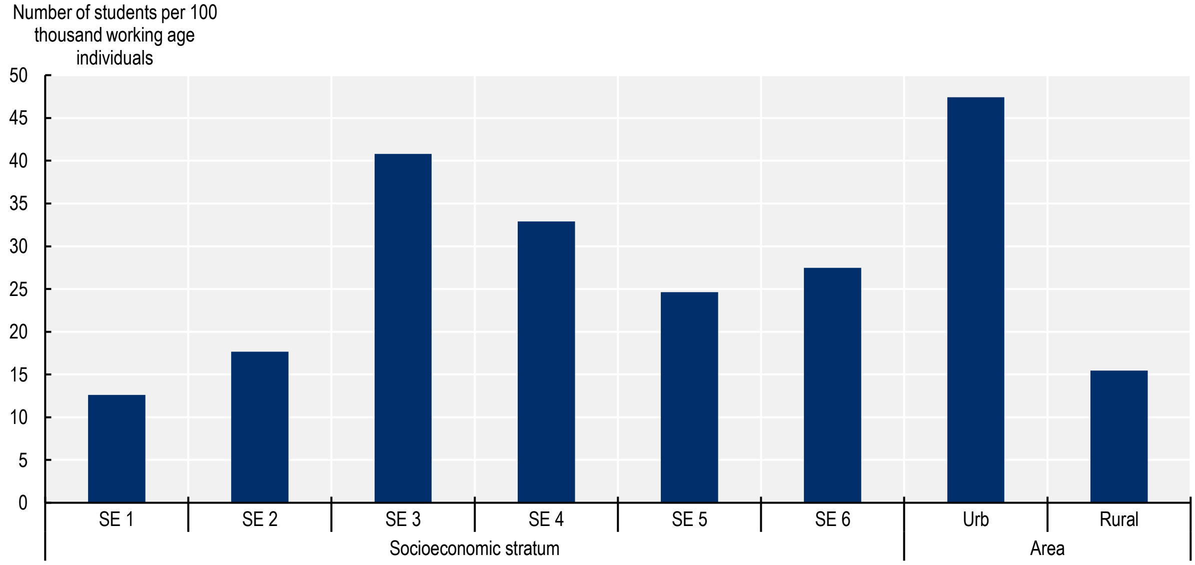
Note: Informatics includes cyber security training. 'Other culture minority' category includes rom, and Raizal from the archipelago. This information is based on the module of Training for employment gathered during the second quarter of 2022.
Source: OECD calculations using Integrated Household Survey 2022 (Gran Encuesta Integrada de Hogares – GEIH), and the module of Training for employment.

The lack of diversity in the cyber security field, particularly regarding gender, may be attributed to stereotypes ingrained in young people from an early age. Such stereotypes and misconceptions about careers in cyber security can influence career expectations and choices, potentially perpetuating current gender diversity imbalances in the profession. In OECD countries, 15-year-old boys are more likely to anticipate working in science and engineering than girls (OECD, 2019[37]). In 2018, the 'ICT professionals' occupation ranked among the top three aspirations for 15-year-old boys in OECD countries, whereas it did not even make the top 10 for girls (OECD, 2020[38]). These gender differences in occupational expectations have remained relatively unchanged since 2000 (OECD, 2019[37]). Equally, the under-representation of girls amongst top performers in science and mathematics can at least partly explain the persistent gender gap in careers in STEM fields – which are often amongst the highest-paying occupations (OECD, 2019[37]).

Regional and socio-economic disparities in cyber security education and training programmes

Socio-economic disparities in cyber security education mirror high levels of inequality in higher education enrolment in general. Students from low-income households are less likely to enrol in undergraduate programmes than their high-income peers, regardless of the field of study (Arias Ortiz, Bornacelly and Elacqua, 2021[39]). Typically, students only need to achieve a minimum score on the SABER 11 national standardised test to be eligible for enrolment in higher education programmes. However, students from disadvantaged backgrounds often do not perform as well on this test, which assesses academic skills and knowledge acquired in secondary school and serves as an entrance exam, as their more advantaged peers (Gómez Soler, Bernal Nisperuza and Herrera Idárraga, 2020[40]). This is mainly due to the low quality of public education that most disadvantaged students are enrolled in, as well as unequal access to supplementary tutoring services for test preparation (Gómez Soler, Bernal Nisperuza and Herrera Idárraga, 2020[40]). Evidence indicates that these students have lower pass rate for the minimum requirements especially in STEM programmes (Londoño-Vélez, Rodríguez and Sánchez, 2020[41]). Moreover, students from lower socio-economic background face multiple additional barriers to enrol in higher education programmes, including limited digital literacy, financial constraints and lack of access to necessary tools such as computer and internet connectivity, preventing them from enrolling (Dialogo Inter-Americano, BID, Worldbank, 2021[42]). Figure 3.7 shows that 13 out of 100 000 working age adults from the lowest socio-economic background (Socio-economic stratum 1) were enrolled in systems engineering programmes, which is half of the chances of students from the highest socio-economic background (Socio-economic stratum 6). Most students enrolled in engineering programmes come from middle income households (Socio-economic stratum 3 and 4). Overall, higher education enrolment has increased in the last two decades in Colombia, especially among the most disadvantage learners, but there are concerns in terms of the quality of education these students engage with (Arias Ortiz, Bornacelly and Elacqua, 2021[39]).

Figure 3.7. Participation rate in system engineering programme by socio-economic characteristics in 2022

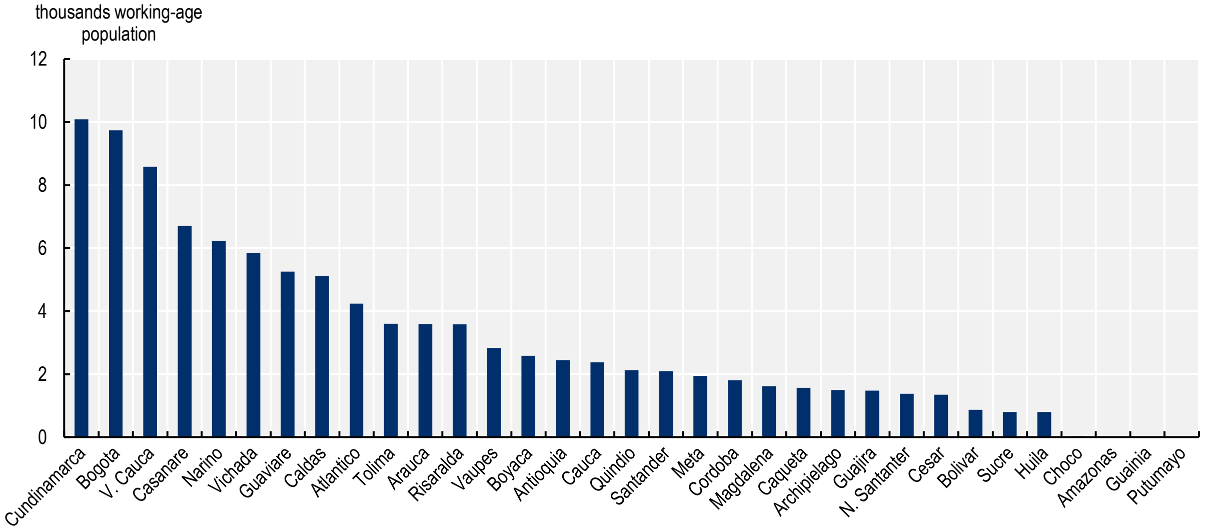


Note: The participation rate is the division between number of students enrolled in system engineering programme from a specific socio-economic stratum/area and the total working-age population from a specific socio-economic stratum/area. Colombia, there are six socio-economic stratum levels (*estratos*) ranging from 1 (Low-Low) to 6 (High), used to classify neighbourhoods and homes for determining utility costs and access to social subsidies. These levels represent different income groups, housing conditions, and access to services and facilities, with lower strata receiving subsidies and higher strata paying higher rates, contributing to the support of lower-income groups.
Source: OECD calculations using Integrated Household Survey 2022 (Gran Encuesta Integrada de Hogares – GEIH), and the module of Training for employment.

There is also a major rural-urban divide in participation in education and training related to cyber security. Only 13% of system engineering students are from rural areas. The system engineering participation rate is 16 students for each 100 000 people in rural areas, compared 47 students for each 100 000 people in urban areas (See Figure 3.7).

Moreover, there are important differences in the provision of and participation in cyber security training programmes by subregion. Participation in non-formal training in cyber security related fields such as informatics is highly concentrated in subregions were the main cities or digital hubs are located such as Bogotá, Cundinamarca, Antioquia (Medellín) and Atlántico (Barranquilla). According to the National Statistics Department (*Departamento Administrativo Nacional de Estadísticas*, DANE), these regions together account for the 47% of total participation in in this field. However, when adjusting participation by subregion’s population, the participation rate shows more heterogeneity (see Figure 3.8). Subregions such as Casanare, Nariño, Vichada and Guaviare, which historically have faced limited provision of learning opportunities, have relatively higher participation rate in training programmes in cyber security related fields. In some of municipalities of these subregions, SENA is the only training provider available. The poorest subregion such as Putumayo and Choco have none or low participation rate in non-formal training in the field of informatics.

Figure 3.8. Participation rate in non-formal training programmes in informatics and related fields by subregions in 2022



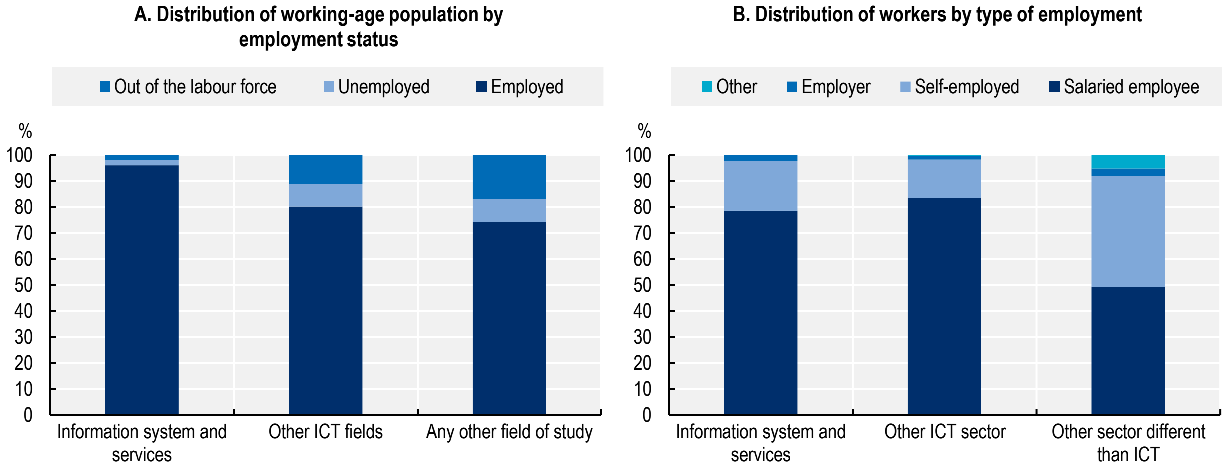
Note: The participation rate is the ratio of the number of students enrolled in informatic non-formal training from a subregion and the total working-age population from a specific subregion.
Source: OECD calculations using Integrated Household Survey 2022 (Gran Encuesta Integrada de Hogares – GEIH), and the module of Training for employment.

Labour market outcomes of cyber security education and training programmes

Employment rate

Individuals with a cyber security degree are more likely to be employed than those with degrees from other fields. In Colombia, 96% of individuals with an information system and services qualification, which includes those specialised in cyber security, are employed. This proportion surpasses that from professionals in other ICT fields (80%) (see Figure 3.9, Panel A). This illustrates the favourable labour market conditions for information system and services professionals in the country. The significant increase of cyberattacks in the last decade has led to considerable surge in demand for cyber security professionals (see Chapter 2). Furthermore, the high employability rate reflects the existing gap in the cyber security workforce. Across Latin America, approximately 500 000 cyber security professionals are needed in the labour market (ISC2, 2022[43]), making it highly probable to find employment opportunities in the field. Most of the information system and services professionals (79%) are employed by companies, organisation, or public institution (see Figure 3.9, Panel B). In contrast, only 19% of professionals in this field work as independent contractors or are self-employed, a share that is significantly lower than workers with degrees in other fields (42%).

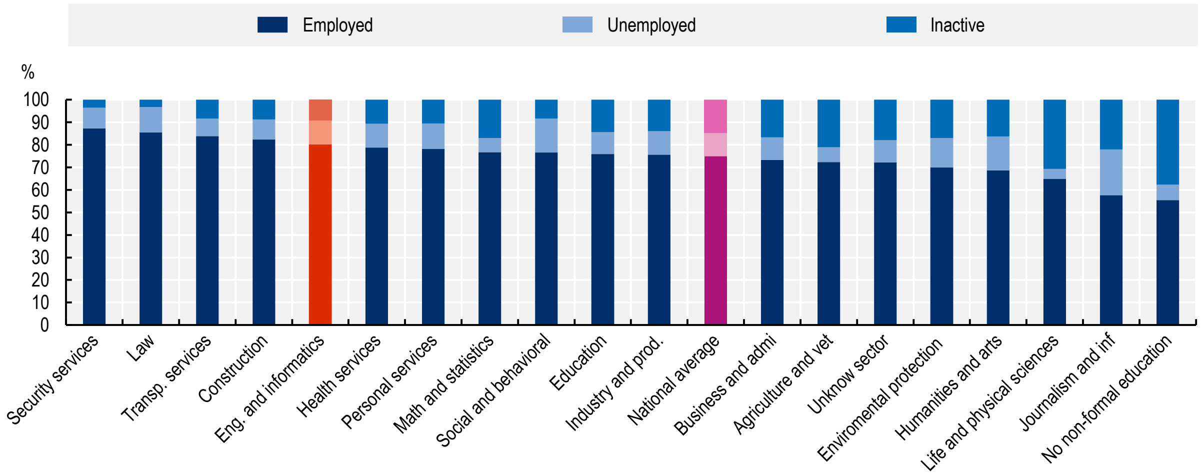
Figure 3.9. Professionals in Information system and services in the labour market in 2022



Note: This figure includes only individuals with professional technical, technologist or undergraduate qualification (ISCED 5 and above). Field of studies reported in the household survey follow the ISCED Classification of level of education and field of studies adapted for Colombia 2011. 'Design and management of information, network and databases' (Code 0612) includes cyber security related fields. The ICT field is identified with code 061 and includes 'Use of computers' (Code 0611) and 'Software and analysis of software and applications' (Code 0613). The category 'Other' includes 'labourers' and 'unpaid workers'. https://www.dane.gov.co/files/sen/normatividad/CINE-N-2011_2019.pdf.
Source: OECD calculations using Integrated Household Survey 2022 (Gran Encuesta Integrada de Hogares – GEIH).

Likewise, individuals who report having participated in non-formal training programmes in engineering and informatics, including cyber security topics, have relatively high employment rates: around 80% of these individuals are employed, which is higher than the national employment rate of 75% (see Figure 3.10). This strong association is also possibly because training participation is typically higher among employed individuals, and in some cases non-formal training is required to start a new position or role. However, practical, hands-on knowledge and expertise in specific, relevant areas are highly valued by employers, particularly in the cyber security field. Obtaining highly sought-after certificates such as EC-Council Ethical Hacker Certificate (CEH), CompTIA+ Security, and Certified Information Systems Security Professional (CISSP), which are highly required by employers in Colombia (See Chapter 2), can significantly enhance employment opportunities according to United States' evidence (Albert, 2017[44]), and help individuals stay ahead in this competitive industry (Castaño-Muñoz and Rodrigues, 2021[45]).

Figure 3.10. Labour market status, by field of non-formal training in 2022



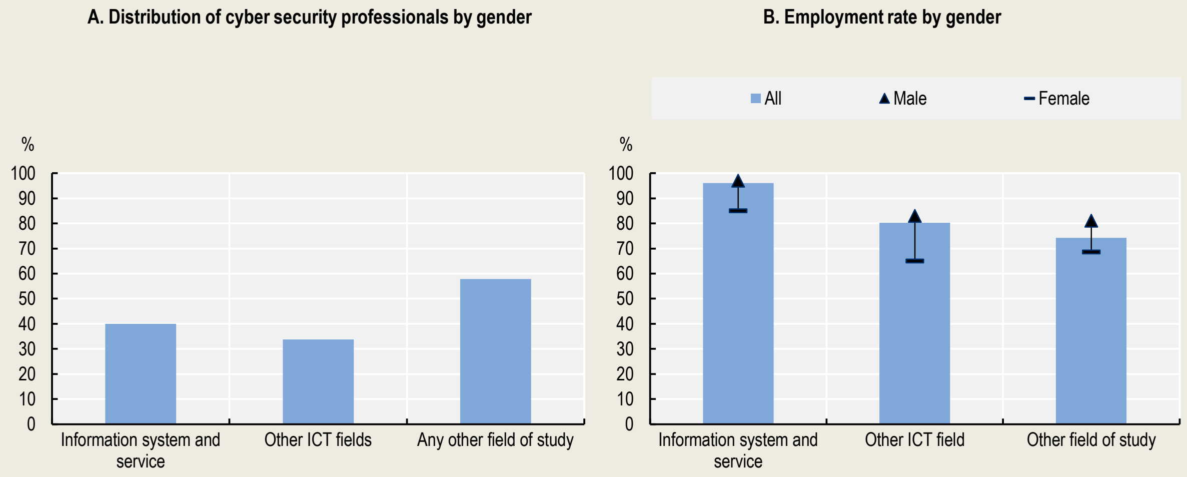
Note: The category 'Information system and services' refers originally to 'Development and management of information systems and information services', which includes cyber security. Degree within the field of 'Information system and services' includes only technical, technologist and university undergraduate programmes. Participation in training in informatics includes people that participated in the 12 months before the time the application of the survey.
Source: OECD calculations using Integrated Household Survey 2022 (*Gran Encuesta Integrada de Hogares* – GEIH).

Employment indicators for women are generally less strong than for men in the cyber security sector (see Box 3.6) Men who hold a cyber security qualification have a higher likelihood of being employed than their female peers. While employment rates for men with cyber security qualifications are higher than for other qualifications, this is not the case for women. However, women with cyber security qualifications do tend to achieve better employment outcomes compared to other ICT sectors. The Colombian Government has implemented policies aimed at diversifying the cyber security workforce and encouraging more young girls be interested in cyber security roles and education (e.g. Hacker Girls), and enrol in STEM courses in general (e.g. Por TIC Mujer) (see Box 3.14). Today, 96% of cyber security professionals are employed, and only 40% of these employed professionals are women, reflecting the still limited participation of women in cyber security education and training programmes.

Box 3.6. Female labour market outcomes in cyber security sector

Despite the government's efforts to diversify the cyber security workforce (as discussed later in this chapter), women in Colombia continue to be underrepresented in this sector. However, the proportion of women working in cyber security is higher than other ICT sectors. Currently, 40% of employed cyber security professionals in the country are women, 14 percentage points higher than in other ICT fields (34%), but significantly lower than in non-ICT fields of study (58%) (See Figure 3.11, Panel A). Women with a cyber security degree, such as system engineering with an emphasis in cyber security, have a lower probability of employment than their male peers, with an employment rate of 85% compared to 97% for men (see Figure 3.11, Panel B). However, the gender difference in the employment rate for cyber security professionals (12 percentage points) is smaller than in other ICT fields (18 percentage points) and in line with the gap observed outside of the ICT field (13 percentage points).

Figure 3.11. Distribution of cyber security workers and employment rate by gender



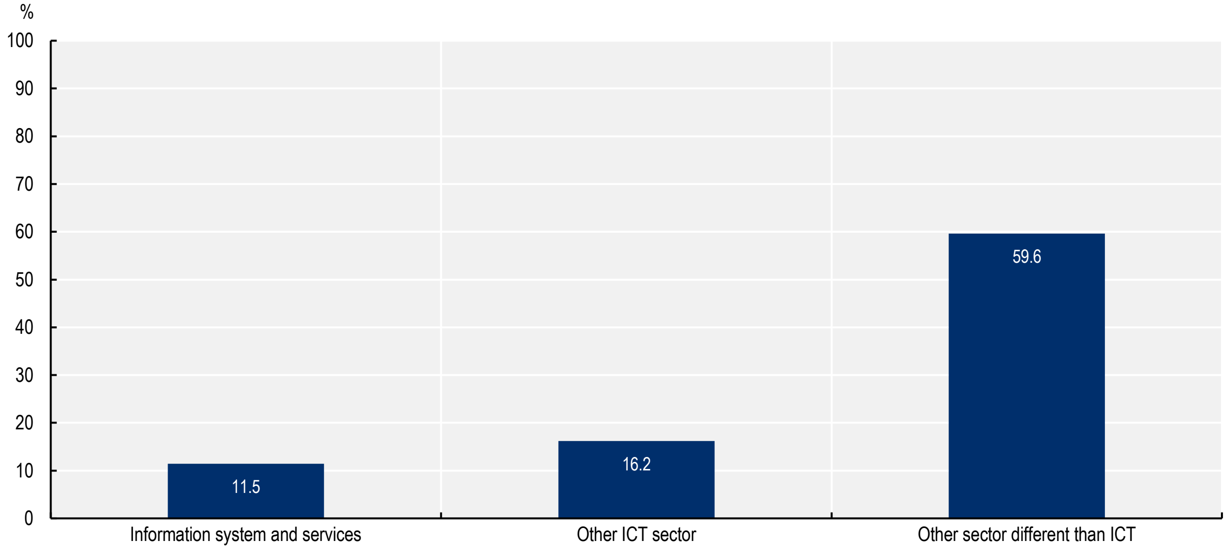
Note: Degree within the field of 'Design and management of information, network and databases' includes only technical, technologist and university undergraduate programmes.
Source: OECD calculations using Integrated Household Survey 2022 (Gran Encuesta Integrada de Hogares – GEIH).

Formality of employment

In Colombia, the ICT sector as a whole demonstrates a high level of human talent absorption, with the majority of workers being employed formally. According to DANE, the proportion of informal workers in the information system and services sector has dropped to 12% in 2022, which is lower than percentage of professional informal workers from other ICT sectors (16%) (Figure 3.12). This trend indicates that the ICT industry, particularly the information system and service field, offers more formal employment opportunities compared to other sectors (see Chapter 2). Some of the factors driving this high level of formality include the increasing digitisation of businesses and public services, rising cyber threats, and growing awareness of the importance of protecting digital assets (OIT, 2022[46])

Figure 3.12. Informality in the information system and services sector vs. other sectors in 2022

Percentage of workers working informally



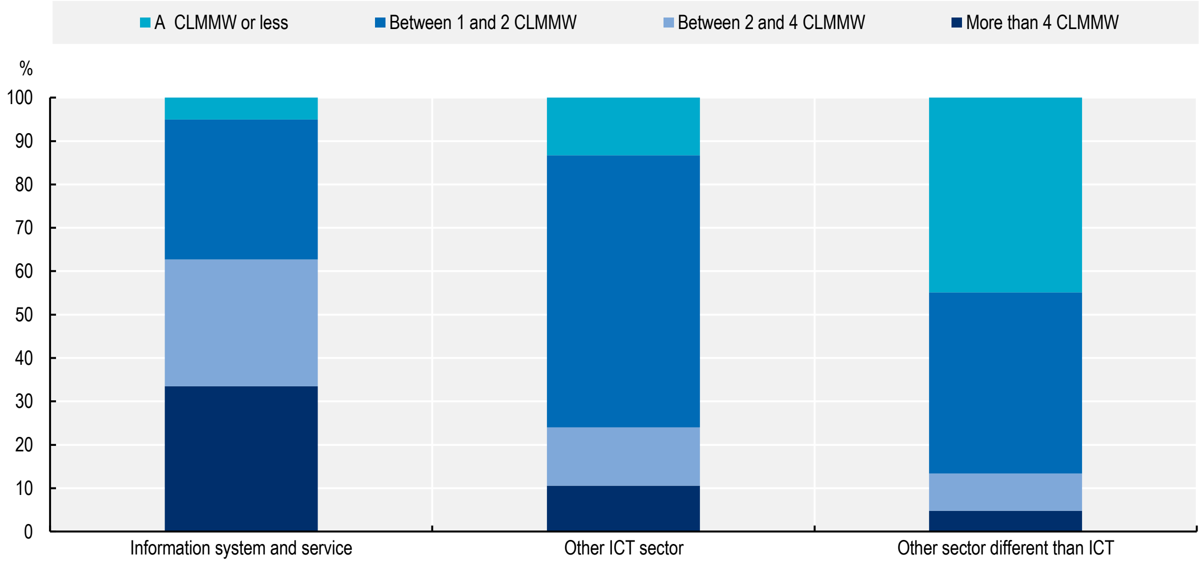
Note: Figures include individuals from all ages and all levels of education. Red line represents the national informality rate in 2022. The category Information systems and services refers originally to 'Development and management of information systems and information services', which includes cyber security. The definition of informal workers follows the National Administrative Department of Statistics (Departamento Nacional de Estadísticas – DANE) guidelines (DANE, 2009[47]). In Colombia, one of the criteria used to define informal employment is linked to access to social security benefits, which include health insurance and the pension system. Workers are considered informal if they do not have a formal contract that ensures their access to these social security benefits. Sectors are identified based on the 2 digits of the International Standard Industrial Classification of all economic activities (ISIC) adapted for Colombia. Development and management systems and information services (code 62 and code 63) includes cyber security related activities. – https://www.dane.gov.co/files/sen/nomenclatura/ciiu/CIIU_Rev_4_AC2020.pdf

Source: OECD calculations using Integrated Household Survey 2022 (Gran Encuesta Integrada de Hogares – GEIH).

Wages

Professionals employed in the information system and services sector in Colombia tend to earn higher salaries compared to workers in the ICT sector as a whole. Figure 3.13 shows that 62% of professionals in information system and services earn more than two times the minimum wage, which is nearly three times higher (24%) than professionals in other ICT sectors and four times higher than (15%) those working in non-ICT sectors. On average a professional in information system and services earned around COP 4 500 000 monthly (approximately EUR 900),[5] which is almost five times the minimum wage in 2022. These relatively high salaries in the cyber security sector indicate a strong demand for skilled professionals in the labour market. Organisations are willing to invest in attracting and retaining top cyber security talent to address cyber security skill gap in the country.

Figure 3.13. Distribution of professionals in information system and services vs. professionals from other sectors, by labour income brackets in 2022



Note: Labour income brackets are defined in terms of Current Labour Market Minimum Wage (CLMMW). Only employees are taken into account in this computation. Sectors are identified based on the 2 digits of the International Standard Industrial Classification of all economic activities (ISIC) adapted for Colombia. Information system and service includes cyber security related activities, https://www.dane.gov.co/files/sen/nomenclatura/ciiu/CIIU_Rev_4_AC2020.pdf.
Source: OECD calculations using Integrated Household Survey 2022 (Gran Encuesta Integrada de Hogares – GEIH).

A framework for dynamic skills development in cyber security

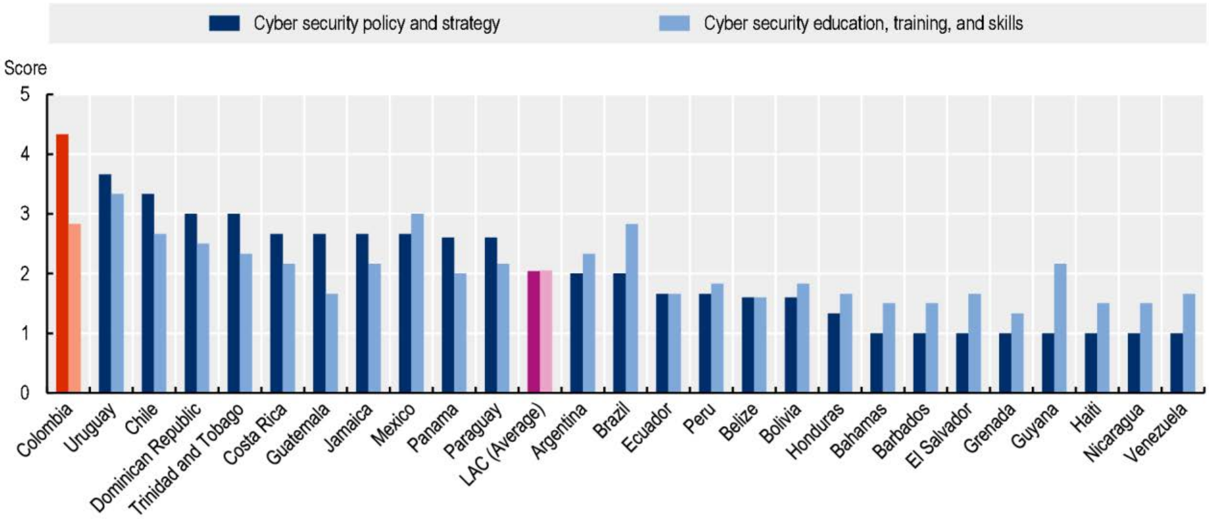
This section first focuses on the overarching policy framework in Colombia, highlighting elements that have sought to enhance cyber security skills in the country. The second part of this section describes how the provision of education and training, in particular within the higher education sector, has responded to the pressure to diversify learning opportunities in this field.

Developing a cyber security policy framework to address skills shortages

While Colombia has a comparatively strong cyber security strategy and policy compared to other Latin American countries, its education and training components are less developed. Within the region, Colombia lags behind countries like Mexico or Brazil in terms of cyber security education, training and skills (Figure 3.14). According to the National Cyber Security Index (NCSI),[6] which measures progress in cyber security policies, including cyber security skills development, Colombia scores 53 points in this skills pillar, well below the OECD average of 87 points (EGA, 2023[48]). The Organization of American States argued that there is a strong need to develop a capacity-building framework and consolidate lines of action that can enhance cyber security education and training (OAS, 2020[49]). In 2020, the first set of clear policy actions was established by MinTIC to provide learning opportunities and increase enrolment in cyber security education (DNP, 2020[50]). Addressing cyber security skill shortages in Colombia requires a multifaceted policy response (OAS, 2023[51]). In particular, it is necessary to raise awareness among stakeholders about the importance of a qualified cyber security workforce and the need to co-ordinate efforts to respond to cyber risk. It is also essential to facilitate the creation of market-led solutions that diversify access to cyber security training and are aligned with labour market needs.

Figure 3.14. Capacity for devising a cyber security strategy and developing cyber security knowledge in LATAM

Score in two dimensions of the cyber security capacity maturity model (1 to 5)



Note: The Cyber security Capacity Maturity Model for Nations (CMM) is a model that aims to assess the maturity level of a country's cyber security capabilities. It identifies five levels of cyber security capacity maturity, with the lowest level indicating an ad hoc capacity and the highest level reflecting a strategic approach with the ability to dynamically adapt or respond to operational, threat, socio-technical, and political considerations. The figure illustrates two out of the five dimensions and provides the arithmetic average of their subdimensions for each dimension.
Source: IDB & OAS (2016[52]), Cyber security: Are we ready in Latin America and the Caribbean?, https://publications.iadb.org/en/cybersecurity-are-we-ready-latin-america-and-caribbean.

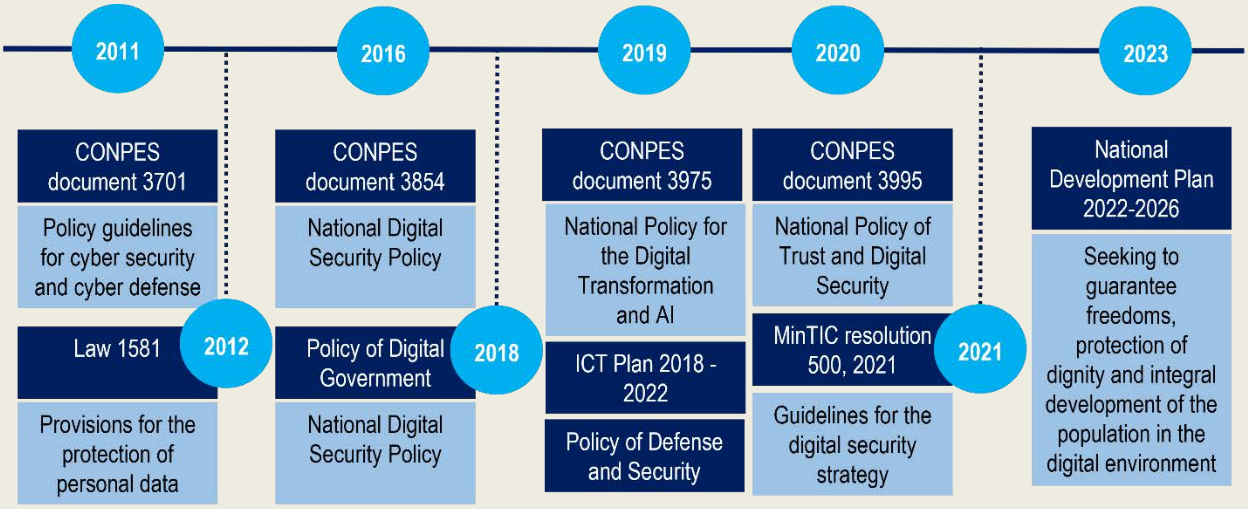
Colombia has enhanced its cyber security policy by adhering to the OECD Policy framework on digital security (OECD, 2022[53]) and the Organization of American States (OAS) guidelines in cyber security policy (OAS, 2023[54]). These two frameworks promote policies that encourage the development of cyber security capabilities. The OECD framework provides guidance for the design of digital security policies, offers recommendations to structure its governance, and establishes strategies to raise awareness about cyber security threats (OECD, 2022[53]). The OAS's approach focuses on delivering policy actions, training, and professional support to member states (OAS, 2022[55]). As part of the Cyber Security Education Action Plan (CEAP), OAS provides guidelines for integrating cyber security into national education plans, as well as a toolkit of best practices to generate interest among learners and encourage employers to provide learning opportunities (OAS, 2020[49]).

Various policy documents have set out strategies regarding the development of cyber security skills in Colombia. The first cyber security and defence strategy, established in 2011, focused on strengthening the country's digital infrastructure against cyber attacks (DNP, 2011[56]). The government provided guidelines to enhance the digital skills of the workforce, including cyber security in 2019 (DNP, 2019[57]). In response, SENA, the Ministry of Education and the Ministry of Labour and Social Protection started to promote cyber security education programmes at all educational levels in 2020. In addition, the MinTIC introduced financial incentives designed to boost participation among various target groups. The incentives were developed following guidelines of the National Council for Economic and Social Policy (Consejo Nacional de Política Económica Social, CONPES). Box 3.7 provides further details of these policy documents.

Box 3.7. Developing a policy framework to enhance cyber security skill policies and strategies in Colombia

Colombia has published several documents to develop national cyber security strategies, including measures regarding the cyber security workforce (see Figure 3.15). Two key documents (CONPES 3701 in 2011 and CONPES 3854 in 2016) were designed to improve the government's capabilities to manage cyber security risk and develop infrastructure for cyber defence (DNP, 2011[56]; 2016[58]). Cyber security skills, however, received limited attention and educational strategies were mainly focused on training in basic preventive measures in cyber security targeting all individuals.

Figure 3.15. Evolution of cyber security policies and strategies implemented by the Colombian Government


2011
CONPES document 3701
Policy guidelines for cyber security and cyber defense
2012
Law 1581
Provisions for the protection of personal data
2016
CONPES document 3854
National Digital Security Policy
2018
Policy of Digital Government
National Digital Security Policy
2019
CONPES document 3975
National Policy for the Digital Transformation and AI
ICT Plan 2018 - 2022
Policy of Defense and Security
2020
CONPES document 3995
National Policy of Trust and Digital Security
MinTIC resolution 500, 2021
2021
Guidelines for the digital security strategy
2023
National Development Plan 2022-2026
Seeking to guarantee freedoms, protection of dignity and integral development of the population in the digital environment

Source: DNP (2020[59]), Política Nacional de Confianza y Seguridad Digital, https://colaboracion.dnp.gov.co/CDT/Conpes/EconpercentageC3%B3micos/3995.pdf; Diaz Acevedo and Cremades Guisado (2023[60]), La evolución de la estrategia de ciberseguridad de Colombia 2011-21, Universidad de Nebrija.

Two additional documents have since sought to address cyber security skill gaps. First, CONPES 3975 was released in 2019. It focused on reducing barriers to digital technology integration, promoting innovation, and strengthening digital skills in the workforce (DNP, 2019[57]). SENA and MEN were designated as the leaders for cyber security education and training programmes. SENA integrates the work of sectorial working groups to design vocational programmes aligned with employers' cyber security skill needs.

Second, in 2020, the DNP and MinTIC prepared CONPES 3995, which emphasised the need to expand learning opportunities in cyber security. It provided guidelines for initiatives to diversify the cyber security workforce, such as increasing participation among women and individuals from vulnerable backgrounds. MEN and MinTIC started to oversee the promotion of cyber security education in higher education institutions, including SENA, with support from international curriculum development experts in this field (DNP, 2020[50]). MinTIC also took responsibility for financial incentives to increase enrolment in cyber security education (DNP, 2020[50]).

Source: Diaz Acevedo and Cremades Guisado (2023[60]), La evolución de la estrategia de ciberseguridad de Colombia 2011-21, Universidad de Nebrija.

In response to the strategy outlined in CONPES 3995 (see Box 3.7), MinTIC has implemented initiatives to raise awareness of cyber security and provide training. The “Digital Skills in Cyber Security” initiative focuses on teaching organisations how to develop prevention and defence strategies and manage risk (MinTIC, 2021[61]). During its first phase in 2021, about 2 000 directors and ICT managers were trained in partnership with Universidad del Norte (see Box 3.8). The same policy document provides guidelines to develop a programme in strengthening enterprises’ digital skills more broadly. For instance, the “Digital Talent” project (*Talento Digital*) provides short-term training in cyber security fundamentals such as protecting sensitive information, managing financial data, and handling personal data (MinTIC, 2022[62]). The objective of this training is to equip employees with the skills needed to ensure operational security (see Box 3.8).

Box 3.8. Translating cyber security policy frameworks into policy actions

Raising awareness of cyber security issues

The MinTIC, through the “Digital skills in cyber security” programme, funds training for employees in enterprises, covering 100% of training expenses (MinTIC, 2021[61]). The programme includes two diploma certificate courses, one for directors and high-level managers, and another for IT managers or IT team leaders. Both cover topics such as risk management, information security, cyberattack prevention and incident response. The programme aims to promote a culture of cyber security and improve the ability of companies to protect themselves against digital risk and threats.

Training employees with relevant digital skills

One of the strands of the Digital Talent programme offered by MinTIC aims to provide training on ICT topics with especial focus on cyber security issues. The programme is oriented mainly to employees of preselected companies. The programme provides full funding, covering technical training, certification exams, and other related expenses. The goal of the programme is to promote the development of digital and cyber security skills within the workforce and to equip them with the skills needed to ensure operational security. This programme helps increase access to education and training for individuals who may not have the financial means to do so otherwise.

Creating a cyber security national learning centre

The government has established a technological development centre (BIOS), focused on applied research, offering services in the areas of biotechnology and data science. Starting from 2023, the MinTIC has allocated COP 7 billion (EUR 1.5 million) to transform BIOS into a specialised national learning centre in cyber security, in line with the recommendations of the Organization of American States. This centre will provide education and training programmes mainly in cyber security covering different level of difficulties, areas of knowledge and taking many forms (e.g. diploma certificates and industry certifications, as well as advanced education programmes such as master degrees). The MinTIC also plans to lead the creation of a transnational centre for the prevention of cybercrime in Latin America.

Source: MinTIC (2021[61]) Equipos de trabajo de 110 empresas recibirán capacitación gratuita en ciberseguridad con el Ministerio TIC, https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/176180: Equipos-de-trabajo-de-110-empresas-recibiran-capacitacion-gratuita-en-ciberseguridad-con-el-Ministerio-TIC-Karen-Abudinen; MinTIC (2022[62]) Proyecto Fortalecimiento de las Competencias Digitales, https://mintic.gov.co/micrositios/convocatoria-habilidades-digitales/775/articles-172269_terminos_Ciberseguridad_2022.pdf Con inversión de $7.000 millones, MinTIC convertirá a Bios en centro formador en ciberseguridad

Diversifying the cyber security offer in higher education

Higher education institutions (HEIs) are increasingly aware of the need to provide programmes and courses that meet the diverse needs of learners and the rapidly evolving skill requirements in the labour market. Colombian HEIs mainly offer formal education programmes as a gateway into cyber security jobs, however, they have been diversifying their offer. The diversification process has involved the development of non-formal programmes such as diploma certificates and other types of short training courses, as well as measures to increase flexibility (e.g. online and hybrid learning options, self-paced modules, and customisable curricula). Non-formal programmes have proven to be more dynamic and adaptable to continuously changing sectors like cyber security, making them well suited to diverse learner profiles.

Short non-formal training courses offered by universities are often recognised and developed in partnership with employers. They allow employers to retrain their employees or fill vacancies. While several current courses in the field of ICT lack an explicit focus on cyber security, they target a broader set of skills within the ICT sector, which may act as foundations for further, more specialised learning. For example, the continuing education department at the University of the Andes has partnered with several companies to develop a range of ICT courses (See Box 3.9). These courses are sometimes included in the regular course offerings, such as micro-credentials that can be recognised and credited towards formal programmes within the same university. Similarly, the engineering department of EAFIT University has recently launched NODO, a flexible learning centre that offers short training courses in ICT (See Box 3.9).

Box 3.9. Designing short training programmes in cyber security with employers

Microcredentials and customised training from Los Andes University

The Continuing Education Department at the University of the Andes provides short programmes or micro-credentials, which are certifiable and verifiable online and cater to the needs of several industries including the ICT sector. These courses cover topics such as software development, coding, and software engineering. Microcredential courses are delivered virtually and are structured by modules, including theoretical learning, as well as workshops and practical problems. The University of the Andes plans to expand its micro-credential offer to include cyber security from 2023 onwards.

Short training courses built with employers by EAFIT University

EAFIT University's Faculty of Engineering has set up NODO, a centre that offers short, flexible training programmes to help young adults learn specific skills required by employers. NODO's distinct learning paths enable students to take on real challenges designed by employers, and acquire an agile skillset that is flexible and adaptable to employer needs. NODO offers a collaborative learning environment where learners can connect technical skills with job related tasks. The first phase of NODO training includes short courses designed and delivered together with employers like Bancolombia, Protección, and SoftwareONE Intergrupo. Currently, NODO offers two learning paths in Web Development and Database Management and plans to develop a new offer in cyber security.

Source: EAFIT university (2023[63]), Nodo: Un ecosistema tecnológico para aprender a desaprender *(Nodo: A technological ecosystem to learn to unlearn),* https://nodoeafit.com/; Universidad de los Andes (2023[64]), Oferta académica de educación continua *(Academic offer of continuing education)*, https://educacioncontinua.uniandes.edu.co/es/programmeas/macro-y-microcredenciales

Industry-led certifications, such as Certified Information Systems Security Professional (CISSP) and Certified Ethical Hacker (CEH), play a key role in signalling skills and underpinning career progression within the field of cyber security (See Chapter 2). Universities therefore sometimes link their non-formal training programmes to industry certifications, so that coursework includes preparation for the relevant exams. For example, the Universidad Distrital de Colombia offers short training courses and preparation for cyber security certifications. Similarly, the Universidad Nacional de Colombia has partnered with Cisco Networking Academy to offer training courses in networking and cyber security (see Box 3.10.)

Box 3.10. Providing short training programmes and granting cyber security certifications

Universidad Distrital de Colombia in partnership with (ISC)2 and EC-council

EUD Academy is a platform developed by Colombia District University that hosts short training courses (about 40 hours of training) preparing for certifications in cyber security. The university has several partnerships with international independent providers such as EC-Council and (ISC)2 to offer company certification training and the assessments to certify individuals' knowledge and competences. EUD offers around 150 certifications with 25 partners including the Certified Information System Security Professional training (CISSP) from (ISC)2, Cyber security ISO/IEC 27032 from ERCA, and CEH from EC-Council. Most companies' certificates require at least five years of experience/ (see Chapter 2). For instance, CISSP prepares students with advanced skills in security and risk management, asset security, security architecture and security operation.

Universidad Nacional and CISCO Networking Academy

The Universidad Nacional has a partnership with CISCO Networking Academy (Netacad) to provide comprehensive learning experience in ICT areas including cyber security. The university is one of the 11 000 institutions around the world where learners can attend in person to participate in the trainings offered by Netacad. Students can pursue training to obtain certifications, such as the Cisco Certified Network Associate (CCNA) and Cisco Certified Network Professional (CCNP). Additional training programmes are available online and in-person, ranging from more basic training such as 'cyber security essentials' and 'introduction to cyber security' to more complex and demanding courses such as 'cloud security' and 'CyberOps Associate'. The Universidad de Nacional offers courses through the faculty of engineering in Bogotá and Medellin. Both branches offer courses in CCNA routing, Switching and CCNA cyber security operations. Over 250 000 students have been trained by the CISCO Academy Netacad, in Colombia. The Netacad programmes has been implemented in various institutions, including universities, technical schools, and vocational training centres, across the country.

Source: Universidad Distrital de Colombia (2023[65]), Curso Certified Information Systems Security Professional (CISSP), https://www.egresadosudistrital.edu.co/index.php/capacitaciones/seguridad-informatica/curso-certified-information-systems-security-professional-cissp

Tackling teacher shortages

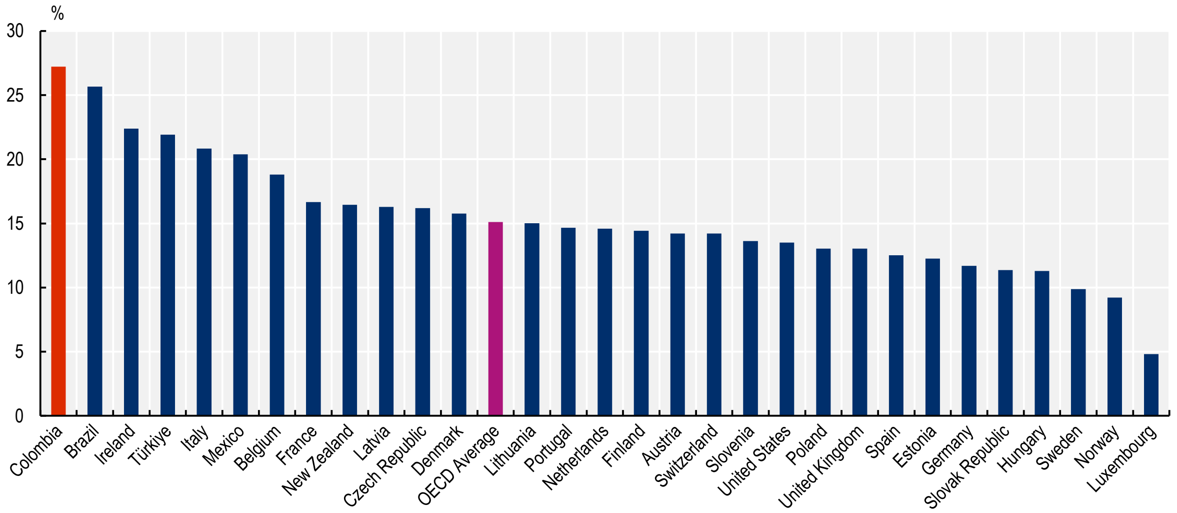
To ensure high-quality cyber security education, the availability of proficient teaching staff is essential. However, Colombia faces a shortage in this field and in the wider ICT sector. This is a major constraint on the provision of education and training programmes. According to DANE, in 2022, over 150 000 teachers and instructors served in higher education institutions, but less than 3% held a degree in an ICT-related field. Only about 200 teachers and instructors have a degree in "information systems and services", which encompasses cyber security.

Across all fields, Colombia has the highest ratio of overall number of students relative to the teaching staff in higher education compared to OECD countries (see Figure 3.16). This high ratio can potentially hinder the quality of education and training (Buckner and Zhang, 2020[66]), damage student engagement and completion (Snijders et al., 2020[67]). Additionally, the number of faculty staff has decreased in recent years, while enrolment in higher education has expanded considerably. Between 2019 and 2021 the number of teaching staff in higher education institutions went from 163 000 to 154 000 (LEE, 2021[68]). Moreover, there are substantial regional differences in the ratio of students per teaching staff which hinder the quality of higher education in some departments. According to the National System of Higher Education

Information (Sistema Nacional de Información de la Educación Superior, SNIES), Arauca and Putumayo, two departments situated in remote areas with limited connectivity and high poverty levels, face the highest student-to-teacher ratios in the country. This exacerbates educational inequalities, disproportionately affecting disadvantaged youth and adults.

Figure 3.16. Students per teaching staff in tertiary education among OECD countries

Ratio of students per teaching staff, 2020 or latest available



Note: The ratio of students per teaching staff is the total number of full-time equivalent students enrolled at a specific level of education divided by the total number of full-time equivalent teachers at the same level. Teachers refer to professional personnel directly involved in teaching students: classroom teachers, special education teachers and other teachers who work with students as a whole class in a classroom, in small groups in a resource room, or in one-to-one teaching inside or outside a regular classroom. This does not include teachers' aides and other paraprofessional personnel.
Source: OECD (2023[69]), Students per teaching staff (indicator), https://doi.org/10.1787/3df7c0a6-en (accessed on 23 June 2023).

Higher education institutions offering cyber security programmes operate in an intensely competitive landscape, vying to retain and attract teachers with up-to-date technical knowledge and skills. They compete not just amongst themselves for the limited full-time academic staff, but also with companies grappling with a shortage of qualified cyber security professionals. Various elements, including remuneration, promotion practices, and leadership style, are pivotal in retaining and attracting professionals to academia, irrespective of the field (Clark, Cluver and Selingo, 2023[70]). However, in most scenarios, higher education institutions lack sufficient leverage to effectively compete with private sector companies.

Attracting and retaining instructors and professors in ICT fields is crucial for expanding the provision of cyber security programmes and reducing the skills gap in the sector. With particular emphasis on technical and technological programmes, as well as short training courses, both the government and educational institutions have sought to strengthen relationships with companies to provide training to ICT teachers. This includes updating their technical skills and improving teaching strategies. Encouraging collaborative strategies between the business sector and higher education institutions (HEIs) is vital to maintaining a pool of qualified educators in cyber security. Some HEIs have fostered partnership that involve instructor training and professional development. For instance, SENA, via the National School of Instructors (*Escuela Nacional de Instructores*, ENI), has established cyber security training programmes for instructors in collaboration with companies (see Box 3.11). Some partnerships focus on teaching specific software packages used in cyber security, alongside broad knowledge in the field, such as ethical hacking.

HEIs also adopt more flexible hiring approaches for professors and instructors, allowing professionals from the industry to dedicate some time to teaching while continuing their employment in companies. In institutions like Pontificia Universidad Javeriana or Universidad EAFIT, this employment arrangement is known as a "lecturer" position (*Profesor de cátedra*), which involves specific subjects and weekly teaching hours. Lecturers receive support from teaching assistants to alleviate academic responsibilities such as grading exams and conducting workshops. Universities leverage their relationships with companies, particularly those managed by their alumni, to invite experts in specific areas to teach courses or modules under this hiring model. According to consulted stakeholders, cyber security professionals who choose to teach as a lecturer are motivated by access to university resources for research (e.g. databases, indexed journals, library facilities, etc.) and the institution's reputation.

Box 3.11. Training trainers in cyber security and other relevant ICT fields: The National School of Instructors

The National School of Instructors (ENI), which operates under the auspices of SENA, is tasked with the training, development, and certification of instructors across an array of vocational and technical fields. Its primary aim is to assure the quality and efficacy of vocational education by equipping instructors with the necessary pedagogical and technical skills. The ENI holds a pivotal role in promoting continuous professional development amongst instructors, fostering innovative teaching techniques, and upholding high education standards within the Colombian vocational training system.

The ENI delivers targeted training for the teaching of ICT, including cyber security programmes. This process includes selecting qualified individuals and developing their pedagogical abilities. Technical training in cyber security is provided to ensure up-to-date knowledge. For instance, certification programmes such as the "Instructor Qualification Route" have already certified around 1 500 instructors in ISO 29001. Collaborations with CISCO and IBM have facilitated a "Cyber security Academy" for instructor certification in networking and computer security. Furthermore, as part of the National Training Plan, instructors have participated in a programme to develop their capacity to deliver courses on digital citizenship. Through these comprehensive approaches, the ENI ensures that its instructors are well-prepared to effectively teach ICT courses, including high quality cyber security education.

Source: SENA (2023[71]), Escuela Nacional de Instructores "Rodolfo Martínez Tono" *(National School of Instructors)*, https://www.sena.edu.co/es-co/comunidades/instructores/Paginas/default.aspx

Improving teachers' English proficiency is also key to ensuring that they can access up-to-date training opportunities. As most significant advancements in this field occur abroad, the latest training is typically available in English. This is a challenge as both learners and teachers often have weak English skills. To address this, the MEN provides English language training as part of the National Bilingualism Programme (MEN, 2022[72]), benefiting schools, higher education institutions, and training providers. Additionally, to enhance English language skills amongst teachers and trainers, training institutions form strategic partnerships. For instance, SENA collaborates with the Heart for Change Foundation, providing English courses facilitated by native-speaking volunteers skilled in teaching English as a foreign language (SENA, 2018[73]). This approach equips instructors with the language skills needed for their professional development.

Access and inclusion in cyber security education and training

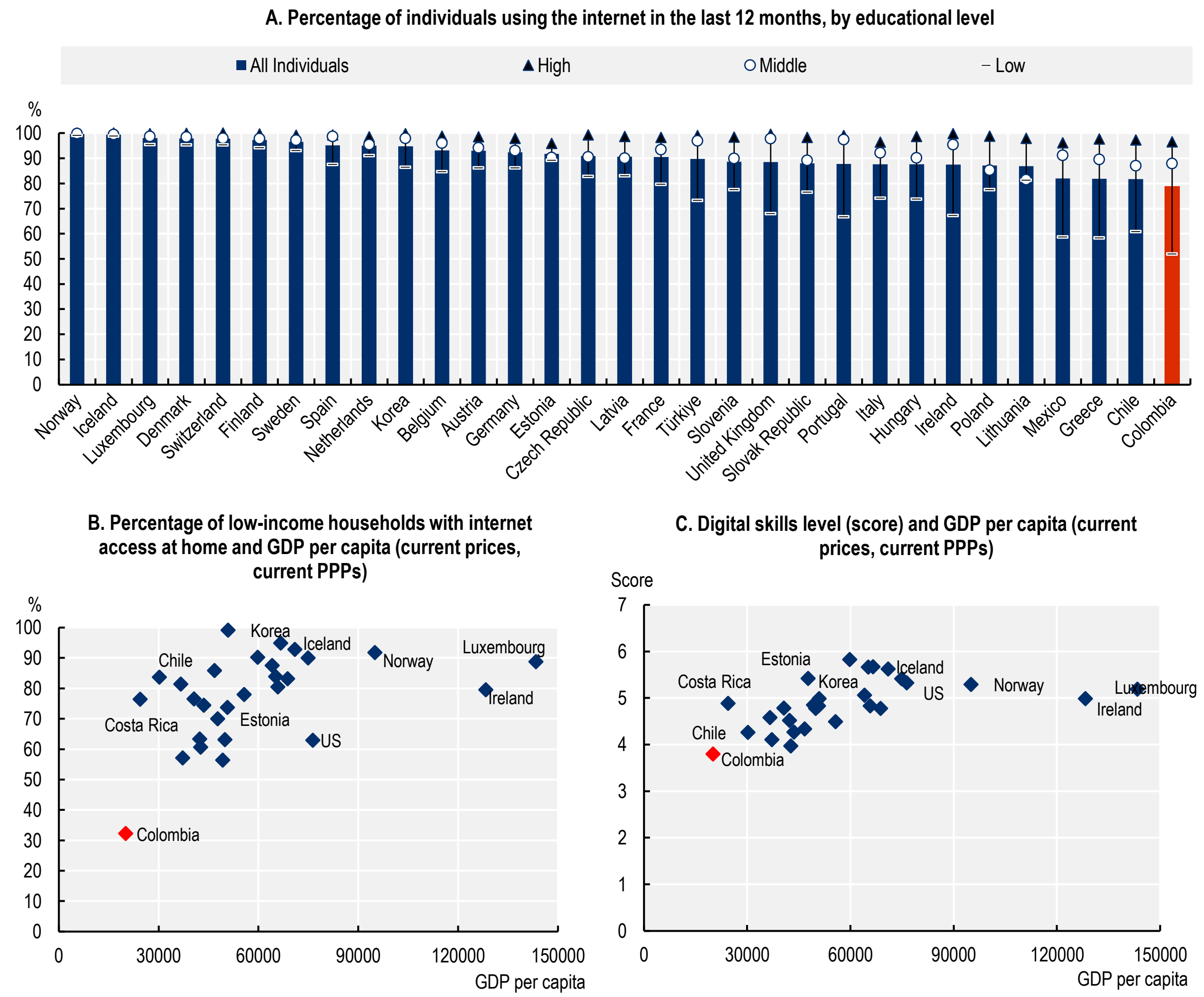
This section focuses on the priority of enabling more learners to access learning opportunities related to cyber security, including the need to increase access among currently underrepresented groups. First, it looks at the importance of developing basic digital skills in the wider population, as a means of raising awareness of cyber security and promoting interest among potential learners to pursue training in this field. Second, it focuses on measures designed to diversify the cyber security workforce by removing barriers that might prevent interested individuals from pursuing learning opportunities.

Tackling digital literacy and raising the interest of potential learners

Participation in cyber security education and training requires individuals to possess solid basic digital skills. Cyber security is a complex field that demands a thorough understanding of various technological tools and systems to facilitate an individual's progress through more advanced training. Furthermore, robust digital proficiency coupled with solid cognitive and problem-solving skills, as well as other competencies necessary for online tasks, are crucial for effectively utilising digital technologies and thriving as a cyber security professional (OECD, 2020[74])

Digital illiteracy is common in Colombia, especially among those from disadvantaged backgrounds. A quarter of computer users are unable to send emails with attachments, and a third are unable to connect other devices (OECD, 2019[75]). Colombia has the lowest percentage of households using the internet (70%) among OECD countries and low network coverage disproportionately affects low-educated individuals and poor households (Figure 3.17, Panel A). The share of low-income households with internet access is below that of countries with similar income levels, like Costa Rica, Chile, or the Slovak Republic (Figure 3.17, Panel B). Such unequal access to technology and their ineffective use undermines efforts to develop digital skills among the population, reinforcing and amplifying existing inequalities and impeding the diversification of the cyber security workforce (OECD, 2020[74]; Van Deursen et al., 2017[76]). According to the World Economic Forum Global Competitiveness Index, the Colombian workforce has one of the lowest levels of digital skills among OECD countries (see Figure 3.17, Panel C).

Figure 3.17. Colombia's internet usage, internet-accessibility and digital skills



A. Percentage of individuals using the internet in the last 12 months, by educational level

B. Percentage of low-income households with internet access at home and GDP per capita (current prices, current PPPs)

C. Digital skills level (score) and GDP per capita (current prices, current PPPs)

Note: Shows countries for which data are available. Categories "High", "middle" and "low" refers to the level of education attained: "higher education and above", "complete upper secondary education" and "less than upper secondary", respectively. The value of the digital skills score shows to what extent the active population possess sufficient digital skills (e.g. computer skills, basic coding, digital reading) ranging between "1", not all, and "7", to a great extent.

Source: OECD (2022[77]), ICT Access and Usage by Household and Individuals (database), https://stats.oecd.org/Index.aspx?DataSetCode=ICT_HH2 (accessed in April 2023); World Economic Forum (2019[78]), Digital skills level among population, Global Competitiveness Report 2020 | World Economic Forum (weforum.org).

In response to these challenges, the Colombian Government has expanded the provision of training programmes covering key fundamental ICT subjects. The MinTIC's website offers free courses and provides certified training on basic digital skills in partnerships with Platzi, CISCO, Microsoft and Google Activate (MinTIC, 2023[79]). These programmes aim to equip learners with basic concepts for digital navigation and facilitate progression to advanced training. Topics covered include, for example, introduction to the "digital learning", "basic informatics in the cloud" and "digital rights and responsibilities". MinTIC also offers a training course on tools and strategies to study online, to support successful completion in online courses.

MinTIC's offer also includes more specialised ICT topics. The 'Talento Digital' website includes basic training for individuals interested in exploring more specialised ICT areas, such as "Introduction to artificial Intelligence", "Introduction to cyber security" and "Fundamentals of cyber security" (see Table 3.8). These courses focus on broader concepts, without complex technical content, and provide a foundation for more advanced programmes. All training programmes offered on MinTic's website are available in Spanish.

Table 3.8. A sample of training programmes in essential topics provided by MinTIC with partners

Name of the training programme	Description	Partner
Basic aspects of Cloud Computing for Developers.	This course covers the basics of cloud computing, including its history, fundamental pillars, and types, as a foundation for real-world practice in Azure. It explores main cloud providers and types of clouds, as well as resources available and economic advantages. It is an essential starting point for developing cloud computing skills, particularly in cyber security.	Microsoft
Introduction to cyber security	This course covers the latest cyber security trends and threats, as well as strategies for staying safe online and protecting personal and business data. It emphasises the importance of cyber security for IT professionals in today's job market. Ideal for those looking to develop their cyber security skills and stay ahead of digital threats.	CISCO Networking Academy
Introduction to the Internet of Things (IoT)	This comprehensive course introduces the transformative impact of the Internet of Things (IoT), including its implications for emerging technologies such as data analytics, artificial intelligence, and cyber security. Participants will learn about the critical role of intent-based networking and software-driven approaches to connecting and securing the billions of new devices emerging every day. Ideal for IT professionals, this course is an essential starting point for exploring the world of IoT and its vast potential.	CISCO Networking Academy
Fundamentals of cyber security	This comprehensive course covers all essential domains of cyber security, including information, system, and network security, ethics and laws, and defense and mitigation techniques. Participants will gain a deeper understanding of cybercrime, security principles, and the latest technologies used to safeguard critical assets. Ideal for IT professionals, this course is an excellent starting point for developing essential skills and knowledge in this rapidly evolving field.	CISCO Networking Academy

Source: MinTIC (2023[79]), Talento Digita – Cursos en línea, https://talentodigital.mintic.gov.co/734/w3-propertyvalue-217941.html (accessed in April 2023).

Several initiatives aim to simulate learners' interest in ICT professions, such as cyber security. The MinTIC has implemented, for instance, initiatives in partnership with the British Council, to develop digital skills among children through fun activities (British Council, 2022[80]) – such as for example the "Code for Kids" project that aims to enhance the programming skills of disadvantaged children from an early age by strengthening the ICT competencies of primary school teachers in public schools and using easy-to-manage devices (MinTIC, 2020[81]). Some initiatives include digital literacy alongside other generic skills, such as soft skills. For example, the Sacúdete initiative (ICBF, 2023[82]) includes training in digital skills and ICT knowledge, as well as mentorship for soft skills development (see Box 3.12). Participants also have access to innovation labs, disruptive technology training, and digital bootcamps. The programme encourages interaction with inspiring young leaders in technology and other sectors.

Box 3.12. Inspiring the most disadvantaged young people in Colombia to engage with 21st-century skills: SACÚDETE programme

Sacúdete is an initiative of the Colombian Institute of Family Welfare (ICBF) to foster 21st-century skills among adolescents and young adults, focusing on both digital skills and transversal abilities (ICBF, 2023[82]). The programme includes three phases: Inspiring, Strengthening, and Transforming. "Inspiring" engages participants in workshops designed to develop digital competencies. "Strengthening" focuses on technical skills with regular ICT classes. "Transforming" involves guidance on further education, employment, or entrepreneurship, helping participants develop and implement their new career plans. Apart from digital and ICT-focused training, Sacúdete includes sessions to enhance critical thinking, assertive communication, leadership, creativity, and empathy.

The programme primarily serves socially, and territorially vulnerable adolescents and young adults aged 14 to 28, providing a differential approach for individuals in rural areas, varying gender and sexual orientations, ethnic backgrounds, and disabilities. Between 2018 and 2022, Sacúdete served about 460 000 young people across nearly 870 municipalities (Consejeria presidencial para la juventud, 2022[83]).

Source: ICBF (2023[82]) Conócenos Sacúdete, https://sacudete.icbf.gov.co/conocenos, (accessed in April, 2023).

Diversifying cyber security workforce by overcoming barriers to access training

Promoting participation in cyber security training also requires removing barriers to access faced by some potential learners – aside from those related to a lack of basic digital skills. High training costs and a lack of financial aid, as well as the predominance of English in online courses (spoken by only 2.5% of Colombians) are major barriers. In response to these challenges, the Colombian Government, trade associations, and the private sector have launched several initiatives to broaden access to cyber security education and training programmes. Efforts concentrate on boosting digital literacy (see above), stirring interest in cyber security education, and offering financial incentives and subsidies, especially to disadvantaged individuals.

The Colombian Government has implemented various initiatives to increase participation in ICT training, including cyber security. The 'Talento Digital' programme provides free certified short courses in fundamental cyber security skills (see above) (MinTIC, 2023[79]). The government also provides scholarships and grants for specialised ICT programmes. For example, the 'One Ticket for the Future' programme (*Un tiquete para el futuro*) provides 90% financing for ICT diplomas, with the remaining 10% covered upon completion (MinTIC and ICETEX, 2022[84]). With this support, individuals can select from 450 ICT programmes across 35 Colombian universities, including 70 programmes focused on cyber security topics such as cryptocurrencies, blockchain, ethical hacking, and cyber security architecture (MinTIC, 2022[27]). All individuals who have already been admitted to any of the programmes included in the ministry's list can potentially benefit from this financing programme. However, up to 50% of the resources will be allocated as a priority to women, students who have been involved in training initiatives provided by the MinTIC, as well as veterans.

Universities and private training providers have also taken steps to improve access to ICT education and training. These initiatives include free courses, mentoring, tutoring and other types of individual support to address students' learning needs. For example, students in the Universidad EAFIT's flexible learning centre (NODO, see Box 3.9) not only receive free training and participate in practical challenges, but also benefit from support by professors and high-achieving students (Box 3.13). Other initiatives adopt a holistic approach, seeking to develop soft skills alongside technical expertise, especially for disadvantaged youth

(Venator and Reeves, 2015[85]). For example, Generation Colombia delivers training in software development, among other topics, and provides courses to develop students' soft skills. The aim is to equip students with the skillset needed to effectively navigate and succeed in the job market (Generation, 2023[86]). Similarly, the District Agency for Higher Education, Science, and Technology (Agencia distrital para la educación superior, la ciencia y la tecnologia, ATENEA) has implemented "Todos a la U", a programme that provide financial support to most disadvantaged young people to engage with short training programmes in ICT offered by public and private universities, complemented with socioemotional skills workshops and courses for learning English (see Box 3.13)

Box 3.13. Providing free learning opportunities to diverse newcomers in the ICT field

NODO, a learning centre designed to broaden access

The Faculty of Engineering at Universidad EAFIT developed NODO, a flexible learning centre that prepares for a career in ICT (see also Box 3.9). The core courses are offered free of charge to the students. Students have the opportunity to explore various learning pathways, composed of modules. These modules encompass a range of topics, from the fundamental aspects of a particular pathway to more specialised and advanced subjects. Depending on their existing knowledge and skills, students have the option to attend levelling classes to ensure a smooth learning progression. Real-life application is at the heart of the learning pathways.

In the first quarter of 2023, Nodo's courses enrolled 93 students, all of whom received funding from seven different organisations. A third of participants were females and 83% came from low-socio-economic households. Most participants were young adults, with 62% aged under 25. It is an objective that by 2026, Nodo will have trained 15 000 students, increased female participant numbers to 45%, and expanded its reach to include learners from rural areas (30%).

"Todos a la U", a programme to overcome multiple barriers

"Todos a la U" is an initiative led by ATENEA, the District Agency for Higher Education, Science, and Technology of Bogota's Mayor's Office, which aims to promote learning pathways in priority sectors in Bogota, including ICT. The programme has three components: learning English, strengthening socioemotional skills, and developing technical skills. Financial support is provided for each component. For the technical skills component, beneficiaries can participate in short training programmes or obtain diploma certificates in areas like video game development, mobile application development, digital design and animation, and user interface and experience design. Training courses in cyber security are planned to be included in the future portfolio.

In its third version launched in 2023, the programme offered 2 400 places for young people in Bogota interested in joining the ICT sector. The programme aims to primarily benefit individuals that belong to disadvantaged groups, including women, individuals from lower socio-economic levels, persons with disabilities, transgender individuals, victims of armed conflict, or individuals in the process of reintegration or reincorporation.

Source: EAFIT (2023[87]), Mientras que algunos resuelven el qué, nosotros creamos el cómo, https://www.eafit.edu.co/nodo, (Accessed, April 2023). ATENEA (2023[88]), Tercera convocatoria Todos a la U, https://agenciaatenea.gov.co/convocatorias/tercera-convocatoria-todos-la-u (Accessed, June, 2023)

Providing training in local languages or offering translation services to ensure that individuals with limited English proficiency can access training can also help broaden access to cyber security training. Weak English skills are a common barrier to participation: only 20% of online short courses in cyber security are available in Spanish (Guo, 2018[89]), while Colombia has one of the lowest levels of English proficiency among LATAM countries (EF, 2022[90]). Addressing this challenge, MinTIC has made sure that all training delivered by public providers is available in Spanish. In addition, the Ministry of Education offers resources for autonomous or guided English language learning through the National Bilingualism Programme, available for different proficiency levels (MEN, 2022[91]).

Barriers are also often linked to a limited understanding and misconceptions of cyber security roles. In that sense, gender stereotypes can hinder participation in cyber security education and training. Girls tend to be less confident in their maths, science and IT competences. This is often fuelled by societal and parental biases, and parents' expectations about the future of their children – independently of performance in mathematics at the age of 15, as measured by the OECD's PISA test (OECD, 2020[38]). This often leads to girls' self-censorship and lower engagement in science and ICTs fields (OECD, 2018[92]). Despite the significant reduction in the performance gap between boys and girls in mathematics and sciences in Colombia (Arias Ortiz and Bornacelly, 2017[93]) and the increasing number of women having complex digital skills (ECLAC, 2022[94]), the proportion of female professionals in ICT is only 23% (ECLAC, 2023[95]). Several initiatives have been implemented to encourage women to engage in education and training in ICT. Examples include the "Hacker girls" programme implemented by MinTIC in Colombia, and regional initiatives, such as LATAM Women in Cyber security (WOMCY) (see Box 3.14 for further details).

Box 3.14. Bringing women into the ICT field and cyber security sector

Hacker girls

The Colombian Government launched in 2015 the programme 'hacker girls', aimed at promoting women's participation in technology and cyber security. The programme provides opportunities for women of all ages to develop knowledge and skills in these fields and to encourage more women to pursue careers in technology and cyber security. Participants receive training through bootcamps, short courses, and engage in challenges using games and simulators. The programme also includes workshops, events and mentorship, connecting women with professionals in the field. The government collaborates with private companies and educational institutions to provide resources and support for the programme.

WOMCY, LATAM Women in Cyber security

WOMCY is a community-driven initiative to promote the participation of women in the cyber security industry throughout Latin America. The organisation provides a platform for support, professional development, and mentorship opportunities. WOMCY offers events, conferences, mentorship programmes, training, and educational resources, and advocates for gender equality in cyber security. This initiative also raises awareness about cyber security issues, including gender-related threats, and exposes participants to activities such as gamification and hackathons to enhance their interest in cyber security careers.

Por TIC Mujer

The "Por TIC Mujer" programme is an initiative in Colombia launched by the MinTIC to enhance women's access to and usage of ICTs. The programme includes various components. Firstly, it offers digital literacy training, enabling women to effectively utilise ICTs. Secondly, the programme improves women's access to technology by providing computers, tablets, and internet connectivity. Finally, it actively supports women in using ICTs for entrepreneurship, offering support through business training and facilitating access to financing opportunities. The ‘Por TIC Mujer’ programme also advocates for gender equality within the ICT sector. By empowering women with the skills, resources, and support they need, the programme aims to create a more inclusive and equitable society, enabling women to thrive in the digital age.

Geek Girls LATAM

Geek girls LATAM focuses on promoting and supporting women in the fields of technology, science, engineering, and mathematics (STEM) across Latin America. The initiative aims to bridge the gender gap in the tech industry by providing a platform for women to connect, learn, and share their experiences in these fields. Geek Girls LATAM leads multiple initiatives, one example is APROPIA, a route of social knowledge appropriation and digital competency strengthening for girls and women in LATAM. This initiative is aimed at women in vulnerable conditions, primarily girls disengaged from armed conflict or unemployed youth interested in enhancing their digital skills.

Source: (MinTIC, 2022[96]), En Colombia más de 20 mil mujeres se formaron con Por TIC Mujer en 2022, https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/273364: En-Colombia-mas-de-20-mil-mujeres-se-formaron-con-Por-TIC-Mujer-en-2022; (GGL, n.d.[97]), Geek Girls LATAM https://geekgirlslatam.org/; (Gobierno Digital, 2022[98]), Hacker Girls, https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Iniciativas/Hacker-Girls/.

References

Albert, K. (2017), “The certification earnings premium: An examination of young workers”, *Social Science Research*, Vol. 63, pp. 138-149, https://doi.org/10.1016/j.ssresearch.2016.09.022. [44]

Alcaldía Mayor de Bogotá (2021), *Fortalecimiento de las competencias de los jóvenes de media del distrito para afrontar los retos del siglo XXI*, https://www.educacionbogota.edu.co/portal_institucional/sites/default/files/2022-02/FICHA%20EBI-D%20PROYECTO%207689.pdf. [9]

Ambito Jurídico (2022), *Los diplomados son cursos de educación informal inferiores a 160 horas que dan lugar a una constancia de asistencia*, https://www.ambitojuridico.com/noticias/general/los-diplomados-son-cursos-de-educacion-informal-inferiores-160-horas-que-dan-lugar. [28]

Arias Ortiz, E. and I. Bornacelly (2017), *Nota CIMA #5: ¿Les va mejor a las niñas en educación?*, Inter-American Development Bank, https://doi.org/10.18235/0001051. [93]

Arias Ortiz, E., I. Bornacelly and G. Elacqua (2021), *Hablemos de política educativa en América Latina y el Caribe #6: Educación superior en América Latina: ¿Cómo las crisis económicas de las últimas décadas han afectado la matrícula?*, Inter-American Development Bank, https://doi.org/10.18235/0003050. [39]

ATENEA (2023), *Tercera convocatoria Todos a la U*, https://agenciaatenea.gov.co/convocatorias/tercera-convocatoria-todos-la-u. [88]

Bonilla-Mejía, L., N. Bottan and A. Ham (2019), “Information policies and higher education choices experimental evidence from Colombia”, *Journal of Behavioral and Experimental Economics*, Vol. 83, p. 101468, https://doi.org/10.1016/j.socec.2019.101468. [36]

British Council (2022), *Programación para niños y niñas*, https://www.britishcouncil.co/instituciones/colegios/programacion-para-ninos-y-ninas. [80]

Buckner, E. and Y. Zhang (2020), “The quantity-quality tradeoff: a cross-national, longitudinal analysis of national student-faculty ratios in higher education”, *Higher Education*, Vol. 82/1, pp. 39-60, https://doi.org/10.1007/s10734-020-00621-3. [66]

Castaño-Muñoz, J. and M. Rodrigues (2021), “Open to MOOCs? Evidence of their impact on labour market outcomes”, *Computers &amp; Education*, Vol. 173, p. 104289, https://doi.org/10.1016/j.compedu.2021.104289. [45]

Clark, C., M. Cluver and J. Selingo (2023), *Talent management becomes a strategy*, https://www2.deloitte.com/us/en/insights/industry/public-sector/articles-on-higher-education/talent-management-in-higher-education.html. [70]

Congreso de Colombia (2002), *Ley 749 de Julio 19 de 2022De la formación y las instituciones de educación superior técnicas profesionales y tecnológicas*, https://www.mineducacion.gov.co/1621/articles-86432_Archivo_pdf.pdf. [23]

Congreso de la República (1994), *Ley General de Educación, Ley 115 de Febrero 8 de 1994.*, https://www.mineducacion.gov.co/1621/articles-85906_archivo_pdf.pdf. [99]

Consejeria presidencial para la juventud (2022), *Con entregatón de 55 infraestructuras Sacúdete, Presidente Duque les cumple a los niños, niñas, adolescentes y jóvenes del país*, https://colombiajoven.gov.co/prensa/con-entregaton-de-55-infraestructuras-sacudete-presidente-duque-les-cumple-a-los-ni%C3%B1os-ni%C3%B1as-adolescentes-y-jovenes#:~:text=Se%20han%20beneficiado%20372.308%20j%C3%B3venes,en%20el%20periodo%202018%2D2022. [83]

CYBERPRO Center (2023), *Javeriana CyberPro Center*, https://javerianacyberpro.com/. [31]

DANE (2022), *Boletín especial: Características de la formación para el trabjo y la educación informal en Colombia*, https://www.dane.gov.co/index.php/estadisticas-por-tema/mercado-laboral/formacion-para-el-trabajo. [24]

DANE (2022), *Formación para el Trabajo - Boletin Técnico*, https://www.dane.gov.co/files/investigaciones/boletines/ech/formacion/GEIH_FormacionTrabajo_abr_jun22.pdf. [25]

DANE (2021), *Clasificación Industrial Internacional Uniforme de todas las actividades económicas*, https://www.dane.gov.co/files/sen/nomenclatura/ciiu/CIIU_Rev_4_AC2021.pdf. [5]

DANE (2018), *Clasificación Internacional Normalizada de la Educación - Campos de educación y formación adaptada para Colombia CINE-F 2013*, https://www.dane.gov.co/files/sen/normatividad/CINE-F-2013-AC.pdf. [4]

DANE (2009), *Metodología informalidad de la Gran Encuesta Integrada de Hogares - GEIH*, https://www.dane.gov.co/files/investigaciones/boletines/ech/ech_informalidad/metodologia_informalidad.pdf. [47]

Departamento Nacional de Planeación (2020), *Documento CONPES - Política Nacional de Confianza y Seguridad Digital*, https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf. [59]

Dialogo Inter-Americano, BID, Worldbank (2021), *El estado de la conectividad educativa en América Latina: Desafios y oportunidades*, https://thedialogue.wpenginepowered.com/wp-content/uploads/2021/11/El-estado-de-la-conectividad-educativa-en-America-Latina-Desafios-y-oportunidades-estrategicas-1.pdf. [42]

Diaz Acevedo, M. and Á. Cremades Guisado (2023), “La evolución de la estrategia de ciberseguridad de Colombia 2011-2021”, *Universidad Nebrija*, https://www.researchgate.net/publication/367043987_La_evolucion_de_la_estrategia_de_ciberseguridad_de_Colombia_2011-2021. [60]

DNP (2020), *Documento CONPES 3995 - Política Nacional de Confianza y Seguridad Digital*, https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf. [50]

DNP (2019), *Documento CONPES 3975 - Política nacional para la transformación digital e inteligencia artificial*, https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3975.pdf. [57]

DNP (2016), *Documento CONPES 3854 - Política Nacional de Seguridad Digital*, https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854_Adenda1.pdf. [58]

DNP (2011), *Documento CONPES 3701 - Lineamientos de política para ciberseguridad y ciberdefensa*, https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf. [56]

EAFIT (2023), *Nodo, mientras que algunos resuelven el qué, nosotros creamos el cómo*, https://www.eafit.edu.co/nodo (accessed on april 2023). [87]

EAFIT university (2023), *Nodo: Un ecosistema tecnológico para aprender a desaprender (Nodo: A technological ecosystem to learn to unlearn)*, https://nodoeafit.com/. [63]

ECLAC (2023), *Gender equality and women's and girls' autonomy in the digital era: contributions of education and digital transformation in Latin America and the Caribbean*, https://repositorio.cepal.org/bitstream/handle/11362/48702/S2300099_en.pdf?sequence=4&isAllowed=y. [95]

ECLAC (2022), *Social Panorama of Latin America and the Caribbean 2022: Transforming education as a basis for sustainable development*, https://www.cepal.org/en/publications/48519-social-panorama-latin-america-and-caribbean-2022-transforming-education-basis. [94]

Edapp (2022), *20 plataformas para crear y aprender online*, https://www.edapp.com/blog/es/20-plataformas-de-cursos-online-gratuitos/. [33]

EF (2022), *EF English Profiency Index*, https://www.ef.com/assetscdn/WIBIwq6RdJvcD9bc8RMd/cefcom-epi-site/reports/2022/ef-epi-2022-english.pdf. [90]

EGA (2023), *National Cyber Security Index*, https://ncsi.ega.ee/ncsi-index/. [48]

El Colombiano (2021), *Las ventajas de los diplomados*, https://www.elcolombiano.com/tendencias/las-ventajas-de-los-diplomados-DN15812067 (accessed on June 2023). [29]

Ferreyra, M. et al. (2017), *At a Crossroads: Higher Education in Latin America and the Caribbean*, World Bank, Washington, DC, https://doi.org/10.1596/978-1-4648-1014-5. [6]

Fortinet (2023), *2023 cyber security skills gap*, https://edu.arrow.com/media/0pld3mup/2023-cybersecurity-skills-gap-report.pdf. [1]

Fundación politécnico Minuto de Dios (2023), *Técnico Profesional en Servicios de Seguridad Informática*, https://tecmd.edu.co/programas_titulados/tecnico-profesional-en-servicios-de-seguridad-informatica/. [11]

Fundación polítécnico Minuto de Dios (2023), *Técnico profesional en servicios de seguridad informática (Professional technician in information security services)*, https://tecmd.edu.co/programas_titulados/tecnico-profesional-en-servicios-de-seguridad-informatica/. [14]

Generation (2023), *Fórmate e impulsa tu carrera profesiona*, https://colombia.generation.org/. [86]

GGL (n.d.), *Geek Girls LatAm*, https://geekgirlslatam.org/ (accessed on 11 September 2023). [97]

Gobierno Digital (2022), *Hacker Girls*, https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Iniciativas/Hacker-Girls/. [98]

Godec, S., L. Archer and E. Dawson (2021), "Interested but not being served: mapping young people's participation in informal STEM education through an equity lens", *Research Papers in Education*, Vol. 37/2, pp. 221-248, https://doi.org/10.1080/02671522.2020.1849365. [34]

Gómez Soler, S., G. Bernal Nisperuza and P. Herrera Idárraga (2020), “Test Preparation and Students’ Performance: The Case of the Colombian High School Exit Exam”, *Cuadernos de Economía*, Vol. 39/79, pp. 31-72, https://doi.org/10.15446/cuad.econ.v39n79.77106. [40]

Guo, P. (2018), “Non-Native English Speakers Learning Computer Programming”, *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, https://doi.org/10.1145/3173574.3173970. [89]

ICBF (2023), *Conócenos Sacúdete*, https://sacudete.icbf.gov.co/. [82]

IDB and OAS (2016), *Cybersecurity: Are We Ready in Latin America and the Caribbean?*, https://publications.iadb.org/en/cybersecurity-are-we-ready-latin-america-and-caribbean. [52]

Institución Universitaria Escolme (2023), *Tecnologo en redes y seguridad informática (Technologist in Network and information security)*, http://www.escolme.edu.co/. [18]

Institución Universitaria Pascual Restrepo (2023), *Tecnología en desarrollo de software (Technologist in Software development)*, https://pascualbravo.edu.co/facultades/facultad-de-ingenieria/programmeas/tecnologia-en-desarrollo-de-software/. [16]

Institución Universitaria Salazar y Herrera (2023), *Tecnologías en sistemas (Technologist in systems)*, https://www.iush.edu.co/es/Universidad/pregrados/escuela-de-ingenierias/tecnologia-sistemas. [15]

Instituto superior de educación social (ISES) (2023), *Técnico profesional en soporte de hardware y software*, https://www.ises.edu.co/soporte-de-hardware-software. [12]

ISC2 (2022), *Cyber security workforce study*, https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx. [43]

LEE (2021), *Datos y Estadísticas*, https://lee.javeriana.edu.co/datos-y-estadisticas. [68]

Londoño-Vélez, J., C. Rodríguez and F. Sánchez (2020), “Upstream and Downstream Impacts of College Merit-Based Financial Aid for Low-Income Students: Ser Pilo Paga in Colombia”, *American Economic Journal: Economic Policy*, Vol. 12/2, pp. 193-227, https://doi.org/10.1257/pol.20180131. [41]

Manpower Group (2022), *Colombia’s 2022 Talent Shortage*, https://go.manpowergroup.com/hubfs/Talent%20Shortage%202022/MPG_2022_TS_Infographic-Colombia.pdf. [3]

Medellin’s Secretary of Education (2022), *Technical upper secondary programmes (Programas de media técnica)*, https://www.medellin.edu.co/secretaria/vivero-del-software/media-tecnica/. [8]

MEN (2023), *Educación Técnica y Tecnológica en Colombia*, https://www.mineducacion.gov.co/portal/micrositios-superior/Educacion-Tecnica-y-Tecnologica/. [13]

MEN (2023), *Sistema Nacional de Información de la Educación Superior – SNIES (National Higher Education Information System)*, https://snies.mineducacion.gov.co/portal/. [7]

MEN (2022), *Programa Nacional de Bilinguismo*, https://educacionrindecuentas.mineducacion.gov.co/pilar-1-educacion-de-calidad/programa-nacional-de-bilinguismo/. [72]

MEN (2022), *Programa Nacional de Bilinguismo (About the National Bilingual Program)*, https://eco.colombiaaprende.edu.co/about-bilingualism/?playlist=55b8e92&video=d3092d9. [91]

MEN (2020), *Educación para el trabajo y desarrollo humano*, https://www.mineducacion.gov.co/1759/articles-355413_recurso_pdf_FAQ.pdf. [30]

MEN (2017), *Formación por ciclos propedéuticos*, https://www.mineducacion.gov.co/portal/Educacion-superior/Informacion-Destacada/196476:Formacion-por-ciclos-propedeuticos. [22]

MEN (2015), *Prácticas: Pasantias y contratos de aprendizaje*, https://www.mineducacion.gov.co/1780/articles-354776_archivo_pdf_Consulta.pdf. [21]

MEN (2015), *Programa Proyecta-T*, https://proyectateherramienta.mineducacion.gov.co/MenVocOcup/. [35]

MinTIC (2023), *Talento Digital - Cursos en linea*, https://talentodigital.mintic.gov.co/734/w3-propertyvalue-217941.html (accessed on April 2023). [79]

MinTIC (2022), *En Colombia más de 20 mil mujeres se formaron con Por TIC Mujer en 2022*, https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/273364:En-Colombia-mas-de-20-mil-mujeres-se-formaron-con-Por-TIC-Mujer-en-2022. [96]

MinTIC (2022), *MinTIC financiará diplomados en ciberseguridad para empresarios y equipos técnicos*, https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/208806:MinTIC-financiara-diplomados-en-ciberseguridad-para-empresarios-y-equipos-tecnicos. [26]

MinTIC (2022), *Proyecto Fortalecimiento de las Competencias Digitales*, https://mintic.gov.co/micrositios/convocatoria-habilidades-digitales/775/articles-172269_terminos_Ciberseguridad_2022.pdf. [62]

MinTIC (2022), *Un ticket para el Futuro*, https://www.mintic.gov.co/micrositios/unticketparaelfuturo/799/w3-channel.html. [27]

MinTIC (2021), *Equipos de trabajo de 110 empresas recibirán capacitación gratuita en ciberseguridad con el Ministerio TIC*, https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/176180:Equipos-de-trabajo-de-110-empresas-recibiran-capacitacion-gratuita-en-ciberseguridad-con-el-Ministerio-TIC-Karen-Abudinen. [61]

MinTIC (2020), *Ministerio TIC y el British Council forman profesores y estudiantes en programación*, https://mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/80650:Ministerio-TIC-y-el-British-Council-forman-profesores-y-estudiantes-en-programacion. [81]

MinTIC and ICETEX (2022), *Créditos condonables para educación en Colombia - Fondo Un ticket para el Futuro Convenio Interadministrativo*, https://web.icetex.gov.co/documents/20122/687162/Texto-de-la-Convocatoria-Diplomados-Fondo-Un-Ticket-para-el-Futuro.pdf. [84]

MNEMO (2022), *SENA y MNEMO inauguran en Colombia el primer centro tecnológico de excelencia y simulación en ciberseguridad de América Latina (SENA and MNEMO launch Colombia's first cybersecurity technology centre of excellence and simulation in Latin America)*, https://www.mnemo.com/sena-mnemo-ciberseguridad/. [32]

OAS (2023), *Practica Guide for CSIRTs*, https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/Guia-CSIRT%202023%20Digital%20ENG.pdf. [54]

OAS (2023), *Reporte sobre el desarrollo de la Fuerza Laboral de ciberseguridad en una era de escasez de talento y habilidades*, https://www.oas.org/es/sms/cicte/docs/Reporte_sobre_el_desarrollo_de_la_fuerza_laboral_de_ciberseguridad_en_una_era_de_escasez_de_talento_y_habilidades.pdf. [51]

OAS (2022), *National Cybersecurity Strategies*, https://www.oas.org/en/sms/cicte/docs/National-Cybersecurity-Strategies-Lessons-learned-and-reflections-ENG.pdf. [55]

OAS (2020), *Cyber security education: Planning for the future through workforce development*, https://www.oas.org/es/sms/cicte/docs/White-Paper-Cybersecurity-Education.pdf. [49]

OECD (2023), *Students per teaching staff* (indicator), https://doi.org/10.1787/3df7c0a6-en (accessed on 23 June 2023). [69]

OECD (2022), *ICT Access and Usage by Households and Individuals (database)*, https://stats.oecd.org/Index.aspx?DataSetCode=ICT_HH2. [77]

OECD (2022), *OECD Policy Framework on Digital Security: Cybersecurity for Prosperity*, OECD Publishing, Paris, https://doi.org/10.1787/a69df866-en. [53]

OECD (2021), *OECD SME and Entrepreneurship Outlook 2021*, OECD Publishing, Paris, https://doi.org/10.1787/97a5bbfe-en. [2]

OECD (2020), *Dream Jobs? Teenagers' career aspirations and the future of work*, https://www.oecd.org/education/dream-jobs-teenagers-career-aspirations-and-the-future-of-work.htm. [38]

OECD (2020), *OECD Digital Economy Outlook 2020*, OECD Publishing, Paris, https://doi.org/10.1787/bb167041-en. [74]

OECD (2019), *OECD Reviews of Digital Transformation: Going Digital in Colombia*, OECD Reviews of Digital Transformation, OECD Publishing, Paris, https://doi.org/10.1787/781185b1-en. [75]

OECD (2019), *PISA 2018 Results (Volume II): Where All Students Can Succeed*, PISA, OECD Publishing, Paris, https://doi.org/10.1787/b5fd1b8f-en. [37]

OECD (2018), *Bridging the digital gender divide*, http://www.oecd.org/digital/bridging-the-digital-gender-divide.pdf. [92]

OECD (2014), "Learning Begets Learning: Adult Participation in Lifelong Education"*, Education Indicators in Focus*, No. 26, OECD Publishing, Paris, https://doi.org/10.1787/5jxsvvmr9z8n-en. [101]

OIT (2022), *OIT destaca el potencial de las tecnologías para impulsar la e-formalización en América Latina*, https://www.ilo.org/americas/sala-de-prensa/WCMS_855184/lang--es/index.htm. [46]

SENA (2023), *Escuela Nacional de Instructores "Rodolfo Martínez Tono" (National School of Instructors)*, https://www.sena.edu.co/es-co/comunidades/instructores/Paginas/default.aspx. [71]

SENA (2023), *Mesas sectoriales. Conectando sectores*, https://www.sena.edu.co/es-co/Empresarios/Paginas/mesasSectoriales.aspx. [10]

SENA (2018), *Escuela Nacional de Instructores - Comunicaciones - Biliinguismos Espanol-Ingles*, https://www.sena.edu.co/es-co/comunidades/instructores/Convocatorias/CONVOCATORIA-BE-LINGUAL-SEGUNDO-SEMESTRE.pdf. [73]

Snijders, I. et al. (2020), "Building bridges in higher education: Student-faculty relationship quality, student engagement, and student loyalty", *International Journal of Educational Research*, Vol. 100, p. 101538, https://doi.org/10.1016/j.ijer.2020.101538. [67]

Unidades tecnológicas de Santander (2023), *Tecnologia en Desarrollo de Sistemas informáticos (Tecnologist in development of informatic systems)*, https://www.uts.edu.co/sitio/tecnologia-en-desarrollo-de-sistemas-informaticos/#1562800770722-cfdcde65-4afc. [17]

Universidad de los Andes (2023), *Oferta académica de educación continua (Academic offer of continuing education)*, https://educacioncontinua.uniandes.edu.co/es. [64]

Universidad de Manizales (2023), *Ingenieria en Seguridad de la información (Information Security Engineering)*, https://umanizales.edu.co/Programa/ingenieria-en-seguridad-de-la-informacion/. [20]

Universidad Distrital de Colombia (2023), *Curso Certified Information Systems Security Professional – CISSP*, https://www.egresadosudistrital.edu.co/index.php/capacitaciones/seguridad-informatica/curso-certified-information-systems-security-professional-cissp. [65]

Universidad Javeriana (2023), *Ingenieria de Sistemas (System engineering)*, https://www.javeriana.edu.co/carrera-ingenieria-de-sistema. [19]

Van Deursen, A. et al. (2017), "The compundness and sequentiality of digital inequality", *International Journal of Communication*, https://ijoc.org/index.php/ijoc/article/view/5739. [76]

Venator, J. and R. Reeves (2015), *Building the soft skills for success*, https://www.brookings.edu/blog/social-mobility-memos/2015/03/18/building-the-soft-skills-for-success/. [85]

Werquin, P. (2010), *Recognising Non-Formal and Informal Learning: Outcomes, Policies and Practices*, OECD Publishing, Paris, https://doi.org/10.1787/9789264063853-en. [100]

World Economic Forum (2019), *Digital skills among population*, https://www.weforum.org/reports/the-global-competitiveness-report-2020/. [78]

Notes

[1] Under Colombian definition, courses such as ‘diploma’, ‘seminar’, or ‘workshop’ that are offered sporadically, and have a duration of less than 160 hours, are considered informal education (Congreso de la República, 1994[99]). According to the OECD definition, these courses are considered part of non-formal education, which is defined as a sustained educational activity that takes place both within and outside educational institutions and caters to individuals of all ages. This includes open or distance learning courses, private lessons, organised sessions for on-the-job training, workshops, or seminars (OECD, 2014[101]; Werquin, 2010[100]). For this report, we use the OECD’s definition of non-formal education.

[2] ETDH refers to education for employability and human development (Educación para el Trabajo y el Desarrollo Humano).

[3] Course cost based on website search of Diploma certificates offered in April 2023. Conversion in euros based on the average Colombian pesos-Euro exchange rate in April 2023.

[4] Micro-credentials are short qualifications that validate competency in a specific skill or knowledge area. They are quick to obtain, focused on targeted learning outcomes, and aligned with industry needs. They offer individuals the opportunity to acquire specialised knowledge without the time commitment required for longer-term educational programmes. Meanwhile, Macro-credentials are comprehensive certifications that encompass a wide range of skills and knowledge. They require longer study periods and indicate higher expertise or qualifications in a specific field. Generally awarded by educational institutions or professional organisations, they may involve degree programmes or professional certifications.

[5] Conversion in euros based on the average Colombian pesos-Euro exchange rate in April 2023.

[6] The National Cyber Security Index is a global live index, which measures the preparedness of countries to prevent cyber threats and manage cyber incidents. The NCSI focuses on measurable aspects of cyber security implemented by the central government: 1) Legislation in force – legal acts, regulations, orders, etc; 2) Established units – existing organisations, departments, etc; 3) Co-operation formats – committees, working groups, etc; and 4) Outcomes – policies, exercises, technologies, websites, programmes, etc.

OECD Skills Studies

Building a Skilled Cyber Security Workforce in Latin America

INSIGHTS FROM CHILE, COLOMBIA AND MEXICO

As societies become increasingly digital, the importance of cyber security has grown significantly for individuals, companies, and nations. The rising number of cyber attacks surpasses the existing defense capabilities, partly due to a shortage of skilled cyber security professionals. This report delves into the analysis of the demand for cyber security experts in Latin America, using information from online job postings in Chile, Colombia, and Mexico. The analysis investigates recent trends in job demand for various cyber security roles, the geographical distribution of cyber security job postings, and the evolving skill requirements in this field. Additionally, the report focuses on the supply side by examining the landscape of cyber security education and training programmes in Colombia. It explores the different types of programmes offered in vocational and higher education, the characteristics of learners enrolled in these programmes, and their outcomes. Lastly, the report examines policies and initiatives implemented in Colombia to enhance the accessibility and relevance of cyber security education and training programmes. This report is part of a broader initiative that examines the evolution of policies and experiences in the cyber security profession around the world.

PRINT ISBN 978-92-64-91890-0
PDF ISBN 978-92-64-43395-3

9 789264 918900