BRIDGING THE GENDER GAP IN CYBERSECURITY:

Addressing Barriers and Expanding Workforce Participation in Latin America

March 2026

GLOBAL CYBERSECURITY FORUM | Duke UNIVERSITY

Acknowledgments

This report is the result of a collaborative research initiative led by Duke University, aimed at advancing understanding of the reasons for – and solutions to – the challenge of women's inclusion in the cybersecurity field across the Latin America region. Duke University would like to thank the Global Cybersecurity Forum (GCF) for its vision, support, and assistance with this project.

We are especially grateful to the women in cybersecurity who generously shared their stories, challenges, and perspectives. Their leadership and resilience are the driving force behind this work.

We would also like to acknowledge the valuable support of local and regional partners who facilitated connections, provided feedback, and helped us better understand the unique contexts across different countries.

We would like to express our deepest gratitude to LACNIC, WOMCY, DigiAmericas, CCLATAM, CERT.ar, Anatel, the National Cybersecurity Agency of Costa Rica (ANCI), the Ministry of Telecommunications of Costa Rica, CyberCluster, the National Cybersecurity Agency of Chile, Hackada, the Dominican Institute of Telecommunications (Indotel), the National Cybersecurity Agency of the Dominican Republic, Silent4business, Ciberamigos, the Mexican Association of Digital Cybersecurity Researchers (AMIDC), the Mexican Association of the Information Technology Industry (AMITI), Asociación de Internet MX, Copa Airlines, the Computer Security Incident Response Team of Panama (CSIRT-Panama), the Cybersecurity Incident Response Center of Paraguay (CERT-PY), MCIO Brasil (Mulheres CIO Brasil), Associação Ser Mulher em Tech, and the many individuals who made this report possible. Further, we would like to thank Paladin Capital for their founding support for the Duke University Cyber Policy Program, without which this work would not be possible. This project reflects collective efforts, thoughtful collaboration, and shared commitment to advancing equity and bridging the workforce gap in cybersecurity.

This research would not have been possible without the tireless efforts of the authors and research team. We would also like to thank the faculty steering committee members – Professors Campbell Tucker, Alessandra Gonzalez, Piero Bonadeo, Juan Carlos Paris – and our collaborators, whose guidance ensured the quality, depth, and regional relevance of this report.

By Professor David Hoffman, Camila Herrera, JD; and contributors Merritt Cahoon, Isabella Delgado, Andre Barajas, Ana Martinez, Alexandra Salazar Anaya, Elitzandra Dominguez, Kelly Yin, Katherine McKenzie and Ishrit Gupta

Contents

Executive Summary 03

Introduction 05

1. Tracing the Shift: Women in Cybersecurity in LATAM Then and Now 08

1.1 Context for the 'Empowering Women to Work in Cybersecurity Is a Win-Win' report 08

1.2 What has stayed the same 09

1.3 What has changed 10

1.4 Career pathways 11

2. Survey Results 12

2.1 Barriers to entering and advancing in the field 12

2.1.1 Student version 12

2.1.2 Industry version 15

2.2 Comparison of female v. male responses 21

2.3 Summary of surveys 21

3. Solutions and Framework for Change 22

3.1 Starting: pipeline and recruitment solutions 22

3.2 Staying: retention solutions 24

3.3 Succeeding: advancement solutions 25

Appendix A: Industry survey questions 27

Appendix B: Student survey questions 32

Endnotes 35

Executive Summary

In today's global economy, the 'workforce gap' or shortage of cybersecurity workers presents a persistent challenge. It threatens economic development, cyber transformation, and the lives of citizens worldwide. These problems are especially acute in Latin America (LATAM), where countries including Brazil and Mexico have some of the world's most serious cybersecurity workforce gaps. Women remain significantly underrepresented - if the obstacles to entering and advancing in this field were overcome, it could help alleviate the gap and strengthen cyber resilience.

This report builds on the 2022 Boston Consulting Group (BCG) and GCF study Empowering Women to Work in Cybersecurity is a Win-Win. This report was based on a global survey of 2,000 female undergraduate students in science, technology, engineering, and mathematics (STEM) fields - alongside a literature review and 20 expert interviews. It offered one of the most comprehensive examinations of the barriers preventing women's full participation in the field. Respondents represented six global regions and 26 countries. The inclusion of 250 students from Latin America provided an important baseline for understanding the region's challenges.[1]

BARRIERS: The 2022 report identified four stages of barriers to women's careers: **Pipeline, Recruitment, Retention, and Advancement.**

The **Pipeline** stage relates to whether there is a sufficient pool of women with the technical skills and interest to fill cybersecurity roles.

Recruitment refers to the hiring process, including interviews and screenings, and ensuring that women are treated equitably.

Retention covers the span of a woman's career, focusing on maintaining inclusive work environments and substantial diversity, equity, and inclusion (DEI) policies. Retention issues often stem from a sense of low belonging and workplace discrimination.

Advancement refers to promoting women into leadership positions in an equitable manner.

These barriers appear at every stage of a woman's cybersecurity career, underscoring the need for comprehensive, systemic strategies that support women from initial interest and recruitment through retention and advancement.

Using survey data collected in 2025 from university students and industry professionals across Latin America. The results reaffirm many of the 2022 insights, while also offering new details of region-specific barriers.

Key findings include:

Pipeline:

- Nearly 50% of students feel uncertain about how to begin a career in cybersecurity
- The talent pipeline is constrained by limited early exposure to STEM education and the absence of visible female role models

Recruitment:

- Hiring processes remain uneven, with many professionals perceiving bias in interview and screening practices
- Women emphasized the need for greater transparency in recruitment and equitable access to entry-level opportunities

Retention:

- Women reported challenges balancing personal and professional responsibilities: in 2025, a significant share of women indicated discomfort with their work-life balance, echoing 2022 findings
- Career growth opportunities, salary and financial benefits, and work–life balance emerged as the top factors influencing job satisfaction

Advancement:

- Women encounter barriers to promotion, including a lack of transparency over the ways in which their work is evaluated
- Both students and professionals emphasized the importance of mentorship in building the skills and confidence needed for leadership

SOLUTIONS: Addressing the workforce gap and women's underrepresentation requires solutions that reflect the specific challenges women face throughout their careers. We propose concerted public policy action implementing a "**Starting, Staying, Succeeding**" framework:

- **Starting:** Creation of pipeline and recruitment solutions, including early STEM engagement, mentorship, and equitable hiring.
- **Staying:** Adoption of retention solutions such as flexible working arrangements, pay equity, and career development support.
- **Succeeding:** Fostering advancement solutions that ensure transparent promotion processes and increase women's representation in leadership.

Together, these recommendations form a roadmap for increasing women's participation in cybersecurity, helping close the broader workforce gap, and decreasing risk for organizations and individuals across the region.

Introduction

Purpose of the study

The objective of this project has been to evaluate the current state of cybersecurity workforce capacity-building in Latin America, with an emphasis on how training, education, and mentorship can serve as critical enablers of innovation.

Global reports on cyber transformation often focus on infrastructure, technology, or financing. This has left a gap in the understanding of the human and institutional capabilities required to design, implement, and sustain these projects in Latin America. The study addresses that gap by analyzing how countries across the region are cultivating talent and skills, and by offering recommendations that can inform governments, regional policymakers, international partners, and academic institutions. The intended audience includes decision-makers who shape cyber transformation policy and governance, as well as organizations providing technical assistance, training, and funding for technology and infrastructure initiatives.

This focus is particularly timely as this global industry continues to face a persistent shortage of skilled workers, with the GCF and BCG 2024 Cybersecurity Workforce Report indicating a workforce gap of 2.8 million.[2] This figure highlights not only the difficulty of filling specialized technical roles, but also the urgent need to develop sustainable talent pipelines. Moreover, the workforce is not only undersized but uneven - women make up 36% of the broader technology workforce but only 24% of the global cybersecurity workforce.[3] These disparities reflect an underinvestment in training, diversity, and mentorship, as countries attempt to build secure, inclusive, and innovative systems.

Previous global and regional reports have acknowledged the importance of workforce development. But there has been limited attention to the specific contexts of Latin America, where global pressures are amplified by local realities. Organisations often lack the resources to hire or retain specialized talent. They face fragmented governance structures and have limited access to technical expertise. This means that sustainable cyber transformation depends less on acquiring advanced technologies - and more on cultivating the human capital needed to use them effectively. However, there are currently limitations in training, in education to embed competencies within institutions, and in mentorship to help cybersecurity professionals use their skills effectively.

Because of these issues, our research has aimed to build on the initial insights of the 2022 report by carrying out a more in-depth regional study to assess the current barriers that prevent women from entering and advancing in the cybersecurity field. The study prioritized broad participation across Latin American countries, with a specific focus on Argentina, Brazil, Chile, Colombia, Costa Rica, the Dominican Republic, Mexico, Panama, and Paraguay, to allow comparative analysis across a diverse region. This report reflects a wide range of experiences, from university students to cybersecurity professionals in a range of industries.

Scope, methodology, and outreach

Between April and July 2025, our research team distributed two versions of the survey - one for industry professionals and another for university students.

The industry version targeted women currently employed in cybersecurity roles across Latin America, although 210 men also responded.[4] It included 40 questions spanning topics such as workers' paths to their current roles, their perceptions of the cybersecurity industry in their country, and the challenges they have faced. The student version targeted those studying cybersecurity or STEM subjects. This shorter version included 18 questions exploring topics such as knowledge of cybersecurity, general interest in pursuing a career in the field, and barriers to entry. A copy of both versions of the survey can be found in the appendices to this report.

To promote broad participation across the region, our researchers targeted and prioritized nine countries, compiling detailed lists of organizations, key stakeholders, and regional associations. These lists included both existing partners and new entities, among them government agencies, with whom we conducted research and initiated collaborative relationships. Established partners helped disseminate the survey by facilitating connections with additional partners who were willing to share the material within their own networks. In addition, a second phase of outreach employed a randomized online panel to reach a broader and more diverse audience across the region. Together, the surveys reached more than 1,500 professionals and more than 1,000 students across 14 Latin American countries (See Figure 1 below).

Country	Industry (%)	Country (%)
Argentina	12.1 %	18.9 %
Brazil	31.2 %	11.3 %
Chile	1.7 %	9.8 %
Colombia	3.4 %	16.2 %
Costa Rica	14.6 %	11.8 %
Dominican Republic	1.4 %	4.3 %
Mexico	27.0 %	17.8 %
Panama	3.0 %	2.2 %
Paraguay	0.4 %	5.9 %
Others (Ecuador, Peru, Guatemala, Venezuela, Honduras)	5.3 %	1.8 %

Figure 1: Countries of survey respondents

The survey results reveal that female cybersecurity professionals in Latin America work in a wide range of sectors. The most common were technology accounting for 29.2%, government with 19%, and finance representing 12.6%. Some of the women who took part work in other areas, including Non-Governmental Organizations, healthcare, energy, telecommunications, education, materials and industrials, consumer goods, and transportation. This highlights the growing relevance of cybersecurity skills beyond the tech sector. As the demand for skilled workers in these other areas grows, it is essential to understand the pathways women take to find, retain, and develop within a job.

The way in which we distributed our survey enabled us to explore the four obstacles mentioned above (Pipeline, Recruitment, Retention, and Advancement) in greater depth. The student version of the survey shed light on the Pipeline barrier, while the industry version enabled us to gather data from professionals with firsthand experience in Recruitment, Retention, and Advancement.

1. Tracing the Shift: Women in Cybersecurity in LATAM Then and Now

1.1 Context for the 'Empowering Women to Work in Cybersecurity Is a Win-Win' report

Attracting women to the cybersecurity workforce is a strategic imperative, as it enhances cyber resilience, strengthens problem-solving through diverse perspectives, and improves business outcomes.[5]

The 2022 report by BCG and GCF drew a critical distinction between access and agency when contextualizing women's underrepresentation in the cybersecurity field, asserting that simply providing women with access to the field is insufficient.

Women often cannot take advantage of accessible opportunities because external factors limit their control over resources and decision-making. Persistent cultural norms, unpaid care responsibilities, and imposter syndrome reduce women's ability to engage fully with opportunities. In 2025, we continue to see this disconnect: in the responses to our survey, women report general knowledge of the field but remain uncertain about how to act on available opportunities.

1.2 What has stayed the same

Results from the 2022 survey disproved the idea that women are completely unaware of cybersecurity – in fact, 82% of those who responded reported having some, or a lot of, knowledge. However, of that number, only 9% claimed 'a lot' of knowledge, which suggests that for the majority, understanding may not be deep. This is despite the finding that the perception of cybersecurity workers was less negative than in the rest of the world.

Similarly, in 2025, most women surveyed indicated at least some familiarity with the field. However, the 2025 findings reaffirmed a lack of deep exposure to cybersecurity as a concrete and attainable career path, which may serve as an early entry barrier for women. Despite having some knowledge, the issue in 2025 remains that many are unaware of specific opportunities and how to pursue them. This reflects the same agency gap identified earlier.

Unlike previous surveys, our student survey specifically asked students to rate their familiarity levels, providing a clearer picture of the gap between basic awareness and deeper understanding of cybersecurity careers. Our 2025 student survey revealed that while approximately 84% of respondents reported some level of familiarity with the field, only 20% described themselves as 'very familiar' and just 6.9% as 'extremely familiar'. The majority reported only slight (31.4%) or moderate (25.3%) familiarity.

Role models and mentorship remain critical. In 2022, 60% of respondents who had some or a lot of knowledge cited encouragement from a role model.[6] In 2025, respondents (67.2%) again highlighted mentorship as key for building valuable skills.

The 2022 results relating to general career priorities were broadly in line with the 2025 findings regarding what women value in a cybersecurity job (see Figure 2 below). In 2022, Latin American women's top three career priorities were securing a high-paying job, making a meaningful contribution to society, and having opportunities for promotion and advancement.[7] In 2025, the factors impacting job satisfaction were career growth opportunities, followed by salary and financial benefits, and work-life balance. Women continue to prioritize upward mobility within a company and financial compensation.

Figure 2: Top three career priorities of women in cybersecurity in LATAM from 2022 to 2025

Most respondents in both 2022 and 2025 said they perceive a gender pay gap in the field. In 2022, 37% regarded cybersecurity as a job in which achieving a work-life balance is difficult, while in 2025, a similar proportion of women in the industry reported feeling either 'somewhat uncomfortable' or 'extremely uncomfortable' in balancing their professional and private lives.[8]

1.3 What has changed

The more expansive approach of the 2025 survey allowed us to explore women's real experiences of the four barriers. While showing consistency with the previous report, these findings offer a more granular understanding of the factors shaping the trajectories of women in the cybersecurity field.

One of the most significant shifts revealed in our data is a decline in women's interest in pursuing cybersecurity careers. While in 2022, 77% of Latin American women expressed such an interest, this figure dropped to 69% in 2025 (see Figure 3, below).

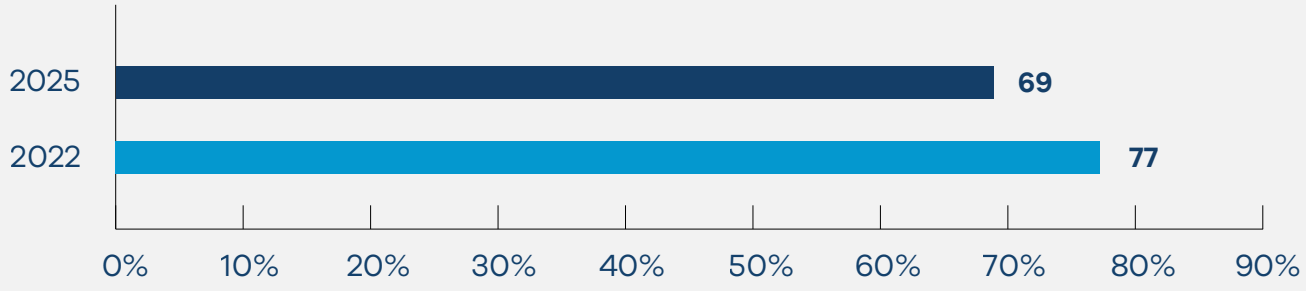


Figure 3: Percentage of women interested in pursuing a career in cybersecurity

This eight percentage point decrease possibly indicates that, despite efforts to raise awareness, there are factors actively discouraging women from viewing cybersecurity as a viable career path. The findings from the 2022 report, together with the data gathered from our 2025 student and industry surveys, present a consistent picture of these challenges and emphasize the urgency of coordinated efforts to close the gender gap.

1.4 Career pathways

To understand the barriers women face, it is important to look at how they typically enter and navigate the cybersecurity field.

In Latin America, there is a growing ecosystem of traditional and non-traditional learning channels.

Traditional entry routes typically begin with a university degree in a STEM field, such as computer science or engineering, followed by a specialization in cybersecurity. These formal pathways allow women with a university STEM background to then specialize in cybersecurity through industry-recognized technical certifications (e.g., Cisco, CCNA) and participation in public-private inclusion programs that offer boot camps, workshops, and gamified learning.

Non-traditional pathways include programs aimed at training women with no formal STEM education backgrounds, including 'Hacker Girls' in Colombia and 'Morras Tics' in Mexico, which offer intensive short-term training and mentorship.[9] Organizations like WOMCY LATAM offer regional mentorship platforms, visibility campaigns, and peer support specifically designed to introduce women without STEM degrees to cybersecurity.[10] Meanwhile, companies such as Cisco, Paladin Capital, and Trellix collaborate with governments and NGOs to deliver resources, training, and job placement to women coming from non-traditional educational backgrounds. For example, initiatives like Cisco's 'Connected and Safe' initiative for Chilean women provide entry points to cybersecurity roles through early exposure, technical skill-building, and teaching sustainability through instructor accreditation.[11] [12] National governments, especially in Colombia and Mexico, have facilitated the development of programs to train and employ women in cybersecurity roles regardless of whether they have a STEM degree or not.

Non-traditional education and training are powerful enablers for women's entry into cybersecurity, particularly in a region where gender gaps in STEM persist. These programs lower barriers to access and offer flexible learning formats, which can enable women to gain in-demand technical and soft skills. They can also establish professional networks crucial for job placement. Beyond technical knowledge, many initiatives also emphasize mentorship and leadership development, which boost women's confidence and visibility in a traditionally male-dominated field. When combined with inclusive recruitment practices and industry partnerships, non-traditional education and training initiatives can significantly expand the pipeline of women ready to enter and advance within Latin America's cybersecurity workforce.

Building on this foundation, it is essential to understand the obstacles that continue to hinder women's participation and progression in the field that were revealed by the 2025 surveys.

2. Survey Results

This section of the report provides a detailed analysis of the 2025 findings, organized around each of the four key barriers—Pipeline, Recruitment, Retention, and Advancement.

2.1 Barriers to entering and advancing in the field

When added to the findings of prior research, the data from our 2025 surveys highlight the complex and persistent barriers faced by women as they try to enter and advance within the cybersecurity field. These challenges can start early – sometimes even before women have seriously considered this field as a career. The barriers may then continue to affect their experiences at every stage of their professional journey. Outlined below are the details of what the two surveys found, showing the similarities and differences between the views of students and those already working in cybersecurity.

2.1.1 Student version

Pipeline

The combination of limited awareness, concerns about work-life balance, and low confidence in their skill sets directly impacts students' motivation and readiness to pursue a career in cybersecurity.

The findings shown in Figure 4 demonstrate significant concerns inhibiting women's interest in pursuing a career in cybersecurity.

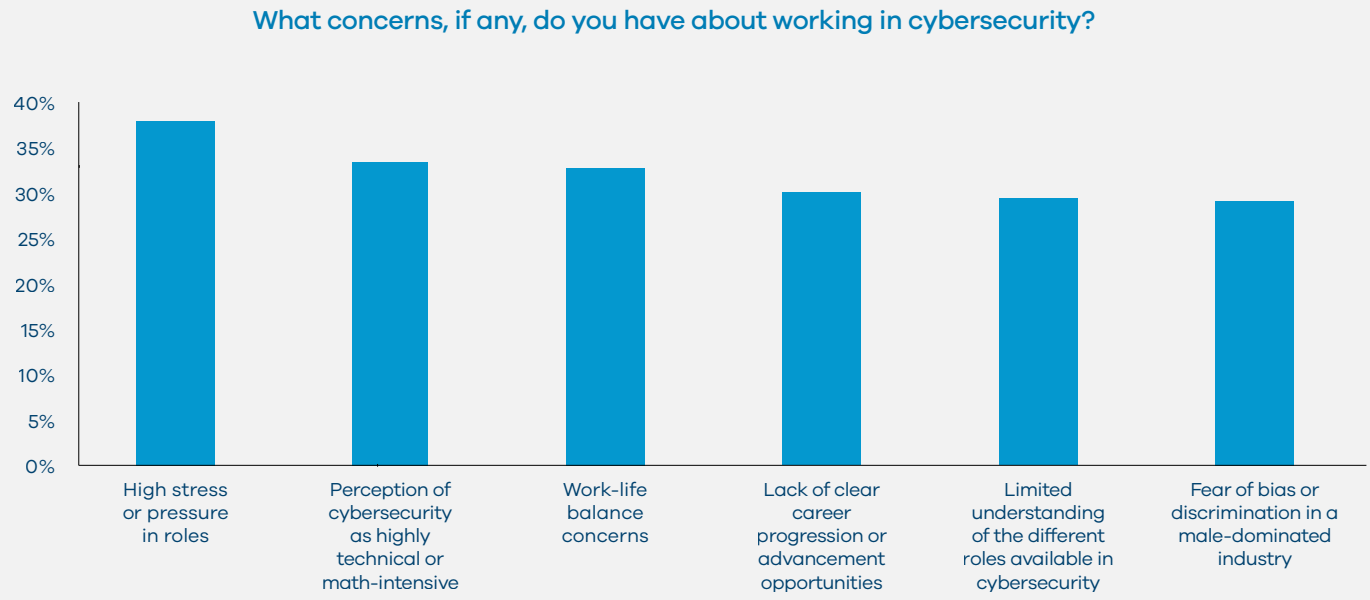


Figure 4: Concerns about working in cybersecurity

Recruitment and retention

Our findings illustrate a recruitment gap between available roles and student awareness of those roles. We also found that students were greatly concerned about the longevity of a career in cybersecurity.

Most respondents identified scholarships or financial aid as the most helpful support for transitioning into cybersecurity, cited by 60.1%, followed by mentorship from professionals at 48.1%. Flexible job options were mentioned by 41.5%, and networking opportunities with other women by 40.4%. A smaller proportion of respondents identified beginner-friendly training, cited by 38.3%, followed by job placements or internships at 28.4% and clearly defined career pathways at 26.2%, while only 4.4% selected other types of resources (see Figure 5 below).

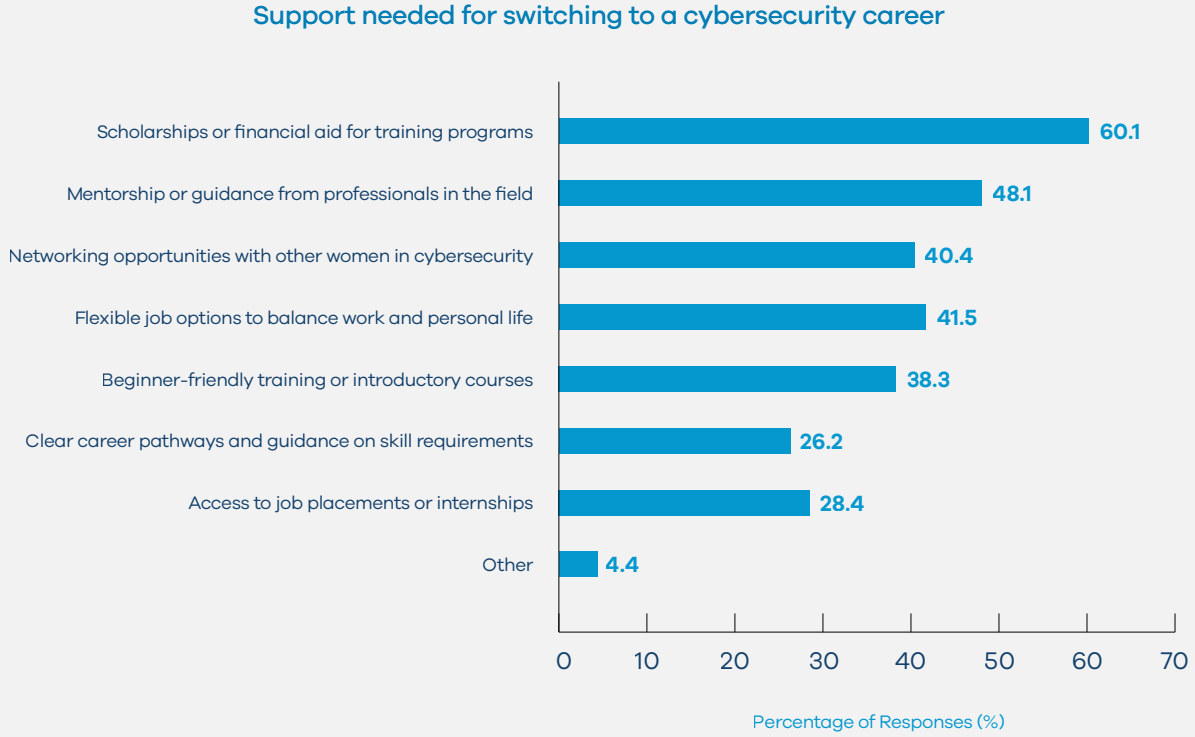


Figure 5: Support needed for students when considering careers in cybersecurity

As Latin American economies expand, so has the demand for positions requiring highly technical skills.[13] Despite these opportunities, our survey revealed that nearly 51% of students felt uncertain about how to begin a career in cybersecurity (see Figure 6 below). This uncertainty suggests that while opportunities exist, they remain difficult to access. This is made harder by other factors such as opaque hiring processes, overly specific qualifications, limited visibility in inclusive spaces, and the absence of structured pathways linking university career services to employers seeking young professionals.[14] This lack of clarity around entry points is compounded by concerns related to skills. 24% of student respondents cited a "lack of confidence in technical skills" as their primary barrier to pursuing a cybersecurity career. Students also highlighted the importance of mentorship and internships, with 26% identifying them as essential for gaining the practical skills and experience needed to enter the field.

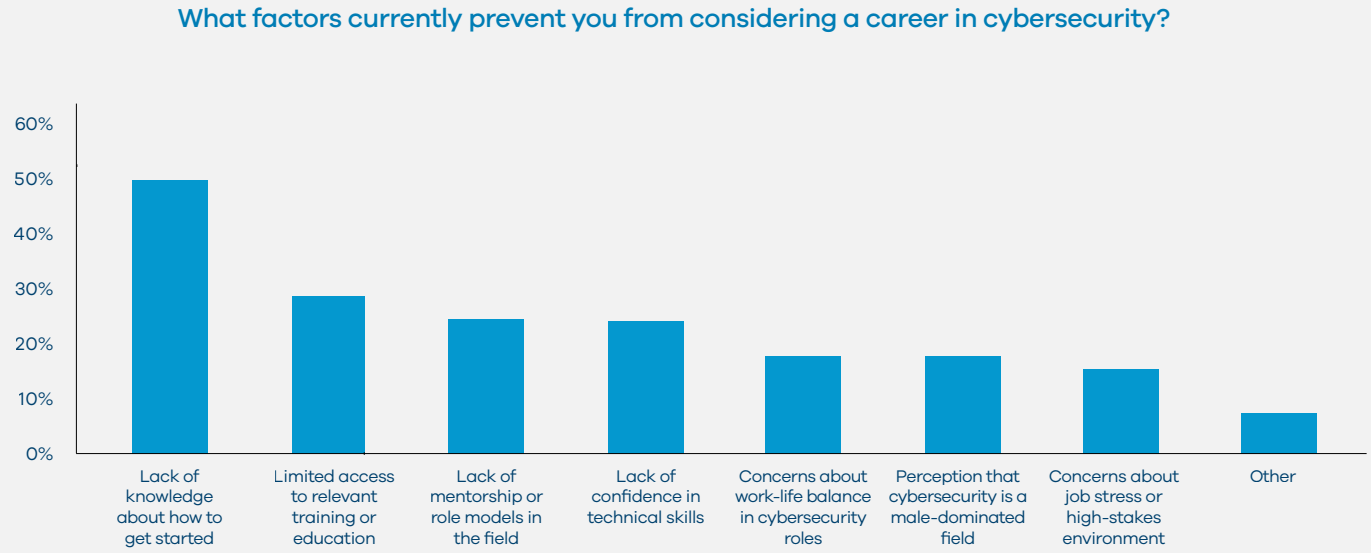


Figure 6: Factors preventing students from considering careers in cybersecurity

Students also expressed concerns about the long-term sustainability of their careers. Roughly 15% were concerned about the high stress or pressure associated with cybersecurity roles, while 33% noted a lack of clear advancement opportunities. These perceptions highlight both recruitment and retention challenges: the industry is often perceived as masculine, complex to access for non-STEM entrants, and demanding to sustain as a long-term career.

Advancement

Advancement of women in leadership roles is paramount to the success of the cybersecurity industry, and the 2025 results show that students are concerned about this even before their careers have begun.

Advancement in cybersecurity requires creating equitable pathways into leadership roles. Survey responses highlighted several barriers that begin even before entry into the field, evidenced at the outset of their potential careers as noted in Figure 4, above. The Figure highlights the primary concerns respondents have about working in cybersecurity.

Together, these findings suggest that beyond technical barriers, cultural and structural factors – such as stress, discrimination, and unclear career trajectories – play a significant role in shaping how individuals view the profession. Addressing these concerns holistically may be crucial to attracting and retaining a more diverse and sustainable workforce.

2.1.2 Industry version

Our research shows that despite growing global demand for cybersecurity talent, women continue to face systemic barriers at every stage in their careers. Many of the concerns highlighted by students – such as fear of gender bias and difficulties in career development – are paralleled by those who responded to the industry survey. These patterns are explored in more depth in the sections below.

Pipeline

In Latin America, while 70% of people are familiar with cybersecurity, only 9% of women report extensive expertise in navigating the field, and 69% of respondents say women are significantly underrepresented in their countries.

Many women see cybersecurity as a male-dominated industry, which further discourages their participation. When asked about the overall representation of women in their countries, 46.7% of respondents said women were 'slightly underrepresented' and 22.4% stated 'very underrepresented' (see Figure 7 below). These perceptions, despite high familiarity, signal that gender bias and discrimination continue to shape women's decisions about whether to enter cybersecurity.

How would you describe the overall representation of women in your country's cybersecurity workforce?

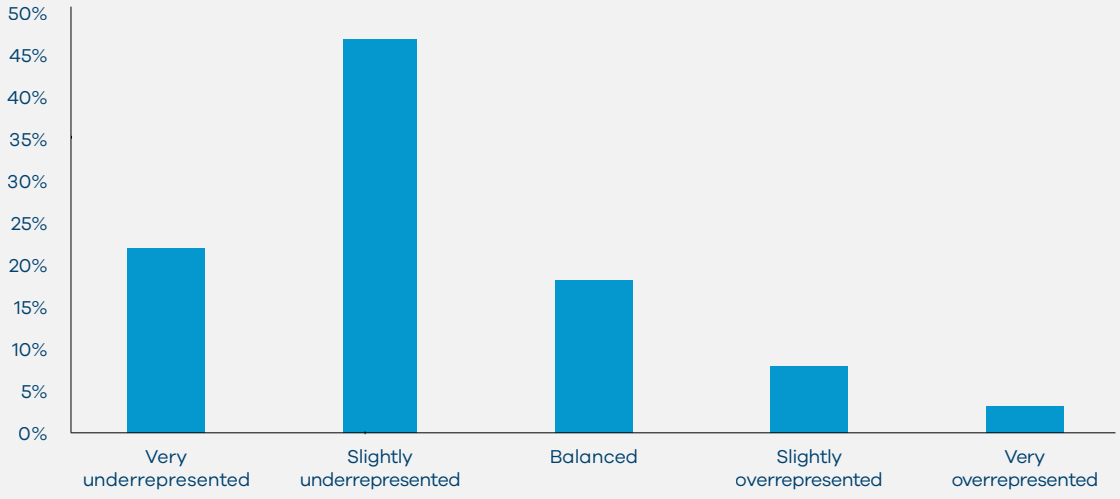


Figure 7: Representation of women in the cybersecurity workforce

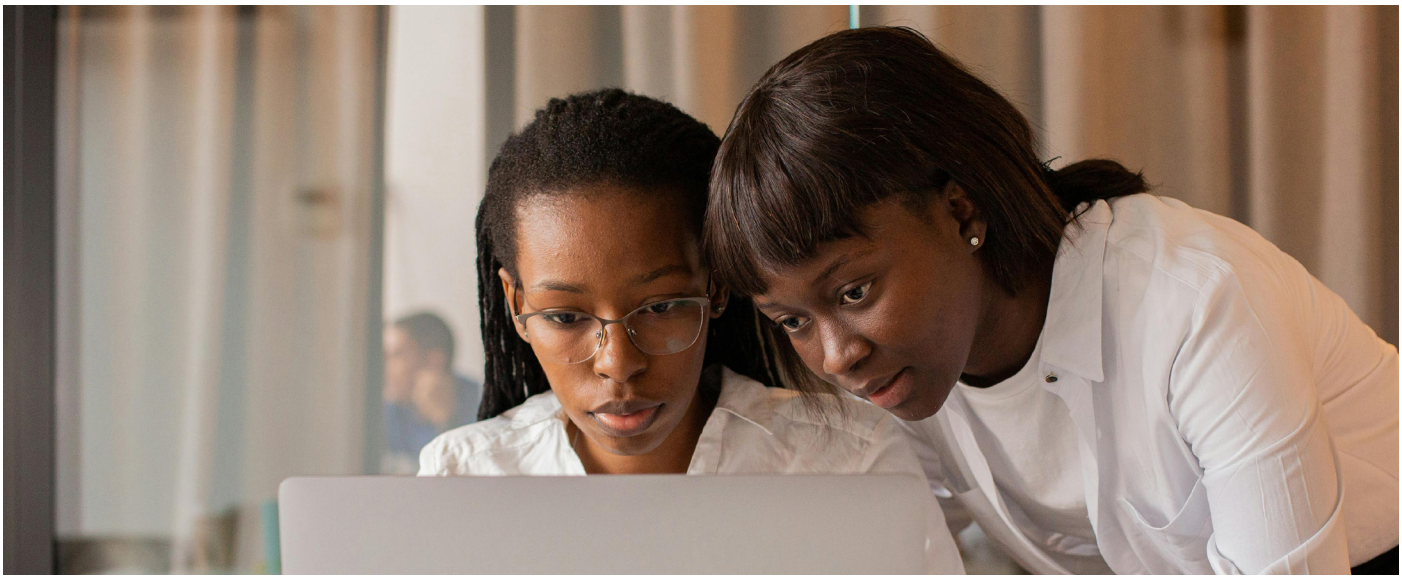
Recruitment

Women in Latin America have traditionally entered the field of cybersecurity through formal STEM pathways. Despite the best efforts of educators, however, university recruitment alone cannot keep up with the industry's needs. Non-traditional pathways are important in fulfilling these demands.

Among women in cybersecurity, our 2025 survey found that 52% entered through non-traditional paths. These alternative pathways reflect a more diverse regional training ecosystem, including short-term workshops, gamified learning experiences, and public-private inclusion programs designed to attract women with no prior STEM education.

One notable example of a successful civil society initiative in Argentina is 'STEM UP!', launched by Global Shapers Buenos Aires to help bridge the gender gap in STEM. This offers a model for how the state can enable strategic change, without necessarily being the sole driver. The program is designed by young leaders and supported by private companies as part of their corporate responsibility objectives. STEM UP! targets women from vulnerable socioeconomic backgrounds—many of them first-generation university students—who face intersecting barriers to their professional development. Implemented in partnership with local universities and the private sector, STEM UP! demonstrates how civil society can deliver agile, context-sensitive responses to inequality, often with a stronger local foundation than centrally planned interventions.[15]

Despite such opportunities, women continue to face significant barriers to entering and advancing in this field. Many respondents reported a lack of training or job opportunities, while technically qualified candidates from non-STEM backgrounds contend with opaque hiring processes and limited entry-level positions. Survey data suggests that these problems are compounded by the effects of gender bias, family responsibilities, lack of visible role models, and limited access to advanced training (see Figure 8 below). Moreover, discrimination remains a significant challenge: 52% of female respondents reported experiencing some form of bias Collectively, these dynamics indicate that while Latin America is building a more inclusive ecosystem of traditional and nontraditional pathways, systemic recruitment barriers and workplace discrimination continue to limit women's full participation in cybersecurity.



What are the biggest challenges women face when entering the cybersecurity field in your region?

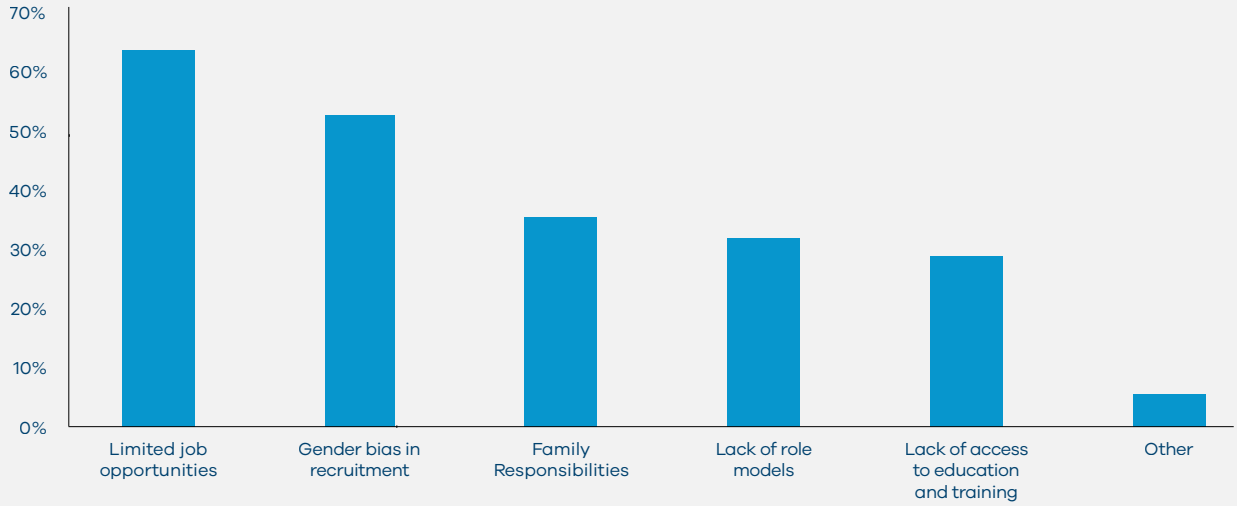


Figure 8: Challenges faced by women entering cybersecurity professions

Retention

Women in cybersecurity continue to face systemic barriers, including workplace bias, exclusion from leadership opportunities, and limited organizational support for gender equity. These challenges are especially pronounced at higher professional levels, where women report discrimination at significantly greater rates.

Retaining women in cybersecurity remains a significant challenge. Many leave the field due to a range of systemic barriers. These include difficulties in taking time off and later reentering the workforce, long working hours, workplace discrimination and bias, limited access to professional development, imposter syndrome, elitism, and a persistent sense of a lack of belonging.

Have you faced any discrimination or bias during your cybersecurity career?

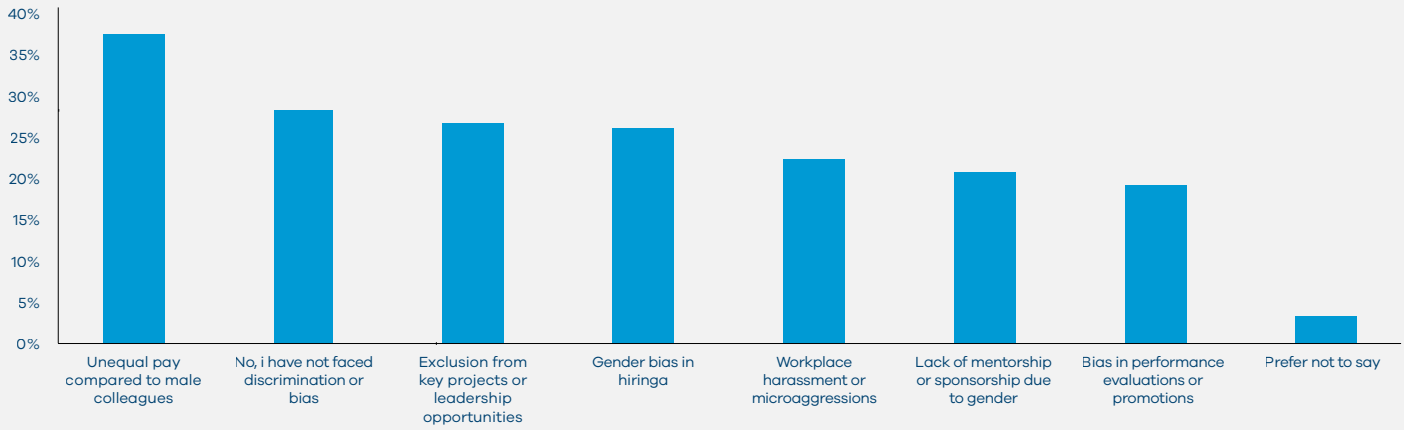


Figure 9: Experiences of discrimination in current cybersecurity roles grouped by professional level

In the 2025 industry survey, women were asked about the types of discrimination they have faced during their cybersecurity careers.

The most frequently reported issue, unequal pay compared to male colleagues, was cited by approximately 38%, signaling systemic inequities that can undermine women's motivation to remain in the field. Similarly, around 27% of respondents reported exclusion from key projects or leadership opportunities, gender bias in hiring, or lack of mentorship or sponsorship, all of which limit career progression and professional recognition (See Figure 9 above).

These barriers often contribute to frustration, slower advancement, and ultimately higher turnover among women. Furthermore, the 23% who cited workplace harassment or microaggressions point to cultural and organizational climates that may feel unwelcoming or unsafe.

Collectively, these findings suggest that addressing bias, pay gaps, and inclusion in leadership pipelines is not only a matter of equity but also essential for improving retention and long-term workforce stability in the cybersecurity sector.

Advancement

Women in cybersecurity face a range of intersecting barriers to advancement. These include limited organizational initiatives, lack of mentorship and role models, family responsibilities, and cultural stereotypes. These systemic challenges restrict progression to leadership roles.

How does your organization promote women's representation and empowerment within cybersecurity roles?

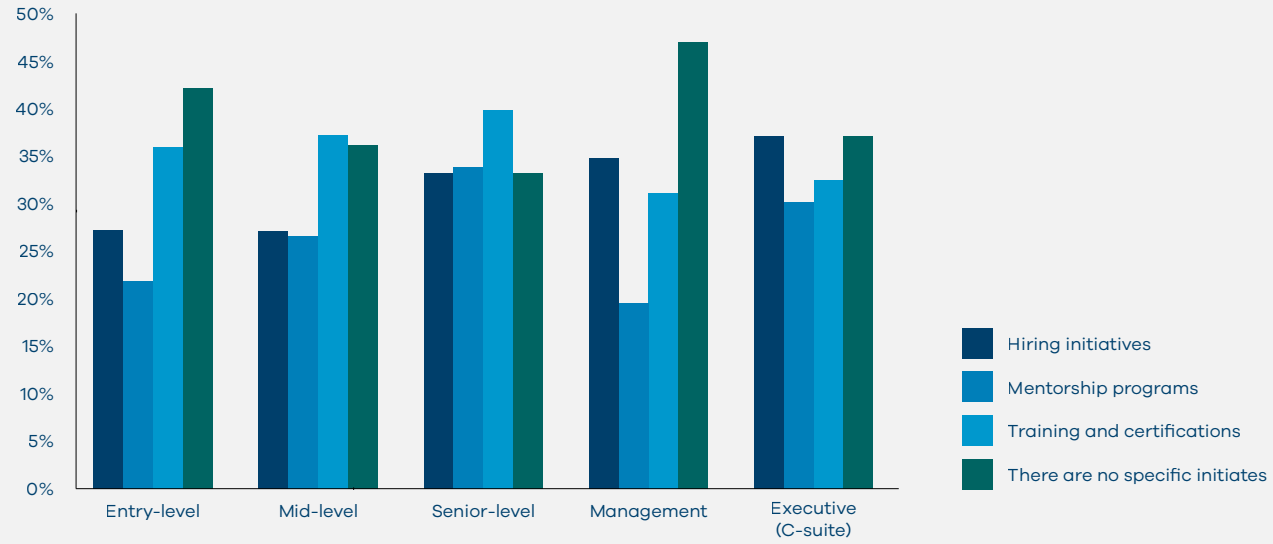


Figure 10: Organizational effort to promote women's representation and empowerment in cybersecurity roles

The data from Figure 10 highlights a troubling gap in organizational support for women in cybersecurity. This is particularly evident at the management level, where 47% of respondents report that their organization does not have any initiatives to advance women—the highest inaction across all career stages. While entry- and senior-level roles see relatively stronger support through training and certifications (36% and 40%), the drop at management indicates a systemic failure to bridge technical expertise and leadership. Even at the executive level, more than one-third of organizations lack targeted initiatives (37%), showing that deliberate strategies for women's advancement remain inconsistent. Overall, organizations invest in recruitment and skill development but struggle to address the critical management transition where many women exit or stagnate in their careers.

The survey offers clear evidence that women in cybersecurity still face significant challenges in career advancement, stemming from a combination of structural, cultural, and organizational barriers. Across industries and organizations, 55% reported a lack of specific initiatives to promote women's representation and empowerment.
In a related question, the survey results provided insight into the barriers specifically faced by women who pursue a non-traditional route to cybersecurity. Among the skills gaps identified, 40% of the women who entered from another field identified a lack of hands-on cybersecurity experience as a barrier. A lack of career transition pathways was mentioned by 22%, while limited access to cybersecurity-specific technical training was identified by 23%.

The difficulty of balancing family responsibilities further hinders career advancement. Women often shoulder a disproportionate share of unpaid labor at home. According to the United Nations Development Programme and UN Women, between 74% to 76% of all unpaid care work in Latin America is done by women.[16] [17] They also face rigid workplace policies that are incompatible with family responsibilities, and which can impede their career progression. Women who took part in the survey, especially those in mid-career, highlighted the challenges of balancing their careers with caregiving responsibilities. Some 36% cited family responsibilities as a barrier to advancing the field (See Figure 8), while 42% said it was challenging to balance family with career advancement (See Figure 11).

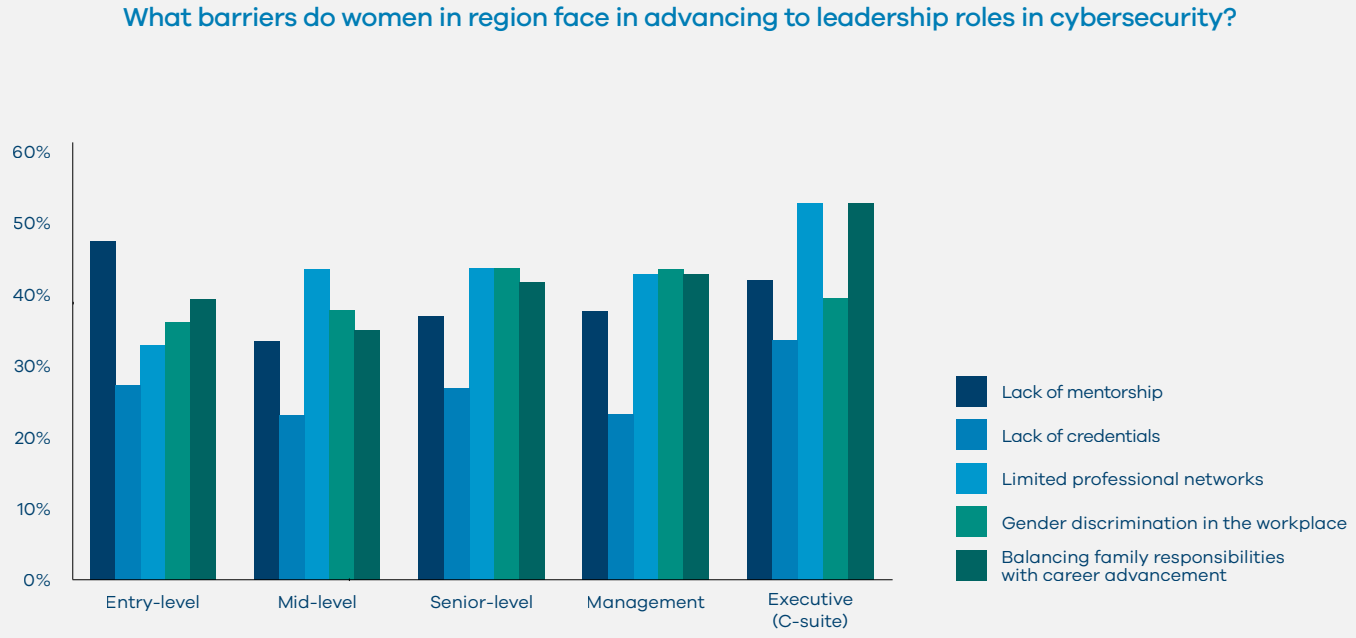


Figure 11: Barriers faced by women advacing to leadership roles

These challenges contribute to, and are reinforced by, the ongoing underrepresentation of women in leadership roles. The scale of this gap is clear: in our survey, more than 60% of participants reported not currently having a mentor. Additionally, 31% of female respondents identified the lack of role models as a barrier to entering the field, and 38% said it prevented women's advancement into leadership roles within the field. Further, persistent gender stereotypes, such as the belief that women are better suited for administrative rather than technical positions, continue to undermine their credibility and limit opportunities within the field.[18] These cultural biases serve as significant barriers to women's full participation and advancement in cybersecurity.

To address these challenges, an overwhelming 78% of respondents emphasized the need for leadership training, followed by 72% calling for formal mentorship programs, 53% for networking opportunities, and 49% for flexible work policies (see Figure 12 below).

What support mechanisms would be most effective in helping women in cybersecurity advance to senior leadership roles?

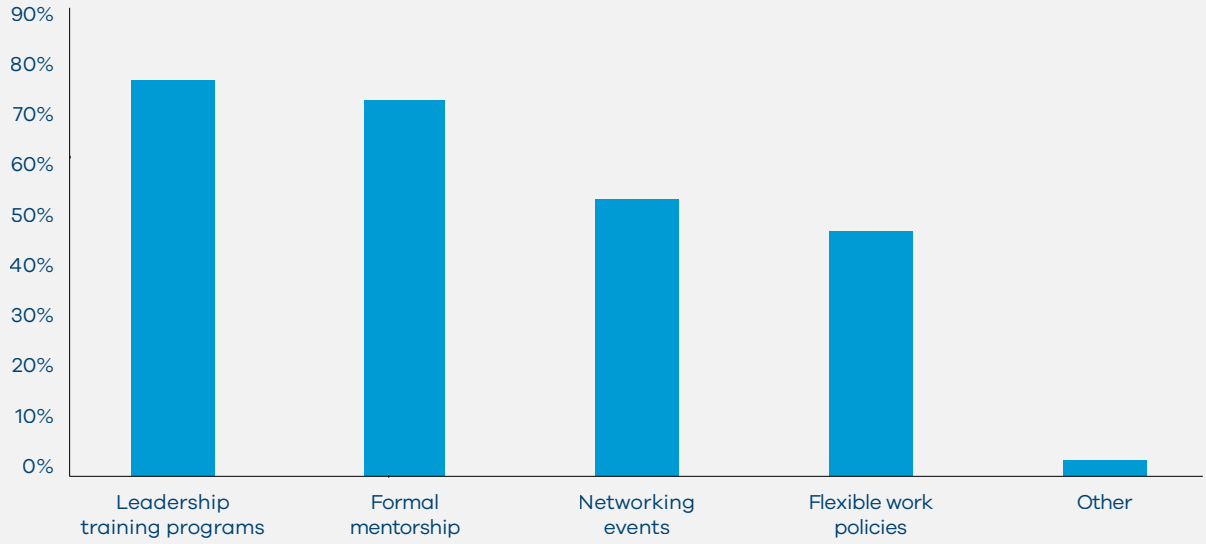


Figure 12: Mechanisms for advancing gender equity in cybersecurity

2.2 Comparison of female v. male responses

Although our surveys focused on women, 210 men also responded to the industry version. This smaller number of male responses limits the reliability of comparisons but does provide some useful insights. On some issues, female and male perspectives differed. But on others, they agreed: around 90% of both men and women agreed that women are significantly underrepresented in cybersecurity. On the issue of pay, only 10% of respondents, both men and women, believed that equal pay exists across the sector.

2.3 Summary of surveys

Identifying and understanding the key obstacles facing women is the first step towards tackling their persistent underrepresentation in the cybersecurity field.

Our 2025 surveys highlight barriers in both the educational and industry settings. This shows a need to raise awareness, encourage meaningful dialogue, and inform future strategies. Our findings underscore the importance of targeted efforts within organizations to create more inclusive environments and to support women's career development in cybersecurity.

3. Solutions and a Framework for Change

Addressing the cybersecurity workforce gap and gender disparities in Latin America requires strategies tailored to the different stages of a woman's career. Our findings confirm that a one-size-fits-all diversity policy is insufficient.

Instead, solutions must respond to shifting barriers. Our approach has three stages, corresponding to the four barrier identified:

- **Starting** (Pipeline and Recruitment)
  - Build stable foundations for women entering cybersecurity
  - Strengthen mentorship and education for workforce transitions
- **Staying** (Retention)
  - Address growth opportunities and benefits
- **Succeeding** (Advancement)
  - Challenge opaque and biased promotion models
  - Increase women's access to leadership roles

This framework recognizes that support and intervention may be necessary throughout a woman's working life. If the gender gap is to be closed, targeted solutions will be needed at every stage—to open doors for women into a cybersecurity career, to ensure that they can thrive, and that they can advance into leadership positions.

3.1 Starting: Pipeline and recruitment solutions

The first step is to ensure that women are actually able to start a career in cybersecurity. Many never get the chance, or are not aware that opportunities exist.

This is due to low STEM engagement, a lack of visible role models, and gender bias in hiring processes.

Recommendation #1: Invest in early talent and training programs

This is a critical first step to building a diverse cybersecurity pipeline. Governments, universities, and industry leaders should expand opportunities for girls and young women to engage with STEM and cybersecurity.

This could be done through school-based coding clubs, summer technology camps, university outreach programs, and initiatives that bring visible female role models into the classroom. Global programs such as Girls Who Code and Technovation provide proven models that can be adapted to regional contexts in Latin America.[19] [20] These initiatives can address the barriers of low awareness, lack of exposure, and the absence of role models. Key stakeholders include ministries of education, universities, and tech companies, with the key audience being girls and young women in primary, secondary, and higher education. Partnerships between schools, universities, and industry can also provide resources, role models, and hands-on learning that make cybersecurity more accessible and appealing at an early age.

Timescale: Short- to medium-term (1–5 years).

Recommendation #2: Establish national cybersecurity apprenticeships

Formal apprenticeships can provide structured entry points for women, especially those transitioning from non-traditional or non-STEM backgrounds.

These apprenticeships should be supported by public–private partnerships, and designed to bridge the gap between academic training and industry employment. They would provide structured, hands-on training and create clear pathways from education to the workplace. They would also would involve ministries of labor, workforce development agencies, universities' career services departments, industry associations, and large employers as key owners. The primary audience would be recent college graduates, and women transitioning careers.

Timescale: Apprenticeships to be designed and piloted over the medium term (3–5 years).

Recommendation #3: Provide mentorship before and during entry level

Targeted mentorship programs in schools and universities would address the persistent lack of visible female role models.

Region-wide alumni networks, and organizations such as Red Ciberlac (the Latin America and the Caribbean Cyber Network), could help fill this gap by connecting students with women in technical and leadership roles who can offer guidance, encouragement, and professional connections.[21] Expanding entry-level access is essential to strengthening the cybersecurity pipeline. Collaborative partnerships among universities, governments, and private companies can create pathways such as internships, apprenticeships, and introductory training programs. To be effective, these initiatives should be geographically inclusive, and designed to reach women from non-traditional backgrounds, including those without prior technical experience.

Timescale: To be initiated in the short term (1-3 years) and sustained in the long term (5+ years).

Together, these measures would address the barrierst of low awareness, lack of role models, and biased recruitment practices, providing a stronger and more equitable foundation for women entering the cybersecurity workforce.

3.2 Staying: Retention solutions

Retention is critical to building a sustainable and diverse workforce. However, our survey shows, that many women who want a long-term career in cybersecurity face serious challenges.

Recommendation #4: Incentivize inclusive workplace policies

Studies show that hybrid options often reduce the "quit rate" of employees, especially for women.[22] To keep women in the cybersecurity workforce, we recommend creating inclusive workplace policies. Employers and policymakers should incentivize practices such as hybrid and remote work options, flexible scheduling, competitive pay structures, and robust parental leave policies.

Policymakers can accelerate adoption through tax incentives or recognition programs for inclusive employers. These policies will directly address workplace inflexibility, caregiving burdens, and persistent gender pay gaps. The stakeholders would include employers, HR leaders, industry associations, and policymakers. Organizations seeking to retain talent would benefit, as would mid-career women who are balancing professional growth with caregiving responsibilities. Where these innovations have been put into practice, studies show that efficiency was maintained over subsequent performance reviews. We urge organizations to adopt hybrid or remote roles, when possible, to help promote industry-wide employee retention.

Timescale: Immediate to medium term (1–5 years).

As an example of a workplace practice which needs to change, 40% of women surveyed indicated that they were paid less than men in the same role—despite the high rate of technological expansion and research which is expected to see the Latin American cybersecurity industry grow to USD 11 billion by 2030.[23]

Recommendation #5: Build regional mentorship and sponsorship networks

Retention also depends on building strong professional networks. Developing mentorship platforms and sponsorship networks will foster confidence in women, enabling them to advance their careers and secure leadership positions.

Mid-career women should be paired with senior professionals who can advocate for their advancement and provide career guidance. Additionally, universities and tech companies should partner with regional associations such as WOMCY to create comprehensive professional development programs. These collaborations should offer industry-recognized certifications in emerging cybersecurity fields. They should also provide executive leadership training tailored to the unique challenges women face in advancing to senior roles. Programs should include flexible learning formats that accommodate caregiving responsibilities. Such partnerships would leverage universities' academic expertise, tech companies' practical industry knowledge, and associations' understanding of gender-specific barriers. Together, they would create targeted curricula that address both technical skills gaps and leadership development needs. These networks can provide mid-career women with access to experienced cybersecurity professionals and essential resources for advancing their careers.

Timescale: To be implemented in the short term (1-3 years) and sustained over the long term (5+ years).

These retention solutions directly address the barriers of workplace inflexibility, pay inequity, and lack of ongoing career support, ensuring that women are not just recruited but also retained in the cybersecurity sector.

3.3 Succeeding: Advancement solutions

Advancing women into leadership positions would have two major benefits: it would break the cycle of bias, and ensure that there are diverse perspectives at the highest levels of cybersecurity decision-making. Advancement practices that replicate existing hierarchies should be reformed.

Recommendation #6: Leadership development and training programs

Women would benefit from investment in specialized leadership development programs. Universities, multinational employers, and training providers should design targeted tracks that prepare women for executive-level positions.

These programs should combine technical upskilling, and management training, as well as peer-learning opportunities that build confidence and increase the visibility of qualified women candidates. Initiatives would target women in mid- to senior-level technical or managerial roles, and would address the barriers of their limited access to leadership preparation, and the low visibility of women who are ready to advance. The programs should be developed and implemented by universities, corporations, and international organizations committed to advancing women in cybersecurity leadership.

Timescale: Medium to long-term (3-7 years).

Recommendation #7: Gender parity and bias-aware promotion in cybersecurity leadership

Organizations should commit to measurable gender parity goals for senior positions and adopt bias-aware promotion practices. This would embed fair selection, and opportunity, and would counter inherent biases which have historically limited the promotion rates of women in cybersecurity.

Traditional recruitment and promotion practices often replicate existing hierarchies and reinforce gendered expectations of management, particularly at upper management levels.[24] To break this cycle, organizations should implement transparent, existing frameworks, such as a Behaviorally Anchored Rating Scale (BARS) or a competency model like the SHRM Competency Model. This can provide a foundation for more objective performance assessments.[25] Many fields have introduced these models to mitigate bias in employee performance assessments and make them more transparent. They should also audit promotion and pay equity data—this would allow them to identify and address disparities.

Timescale: Short-term accountability measures, such as regular reporting, should be introduced to enable long-term systemic change over a 5-10 year period.

These measures directly address bias in promotion practices and the persistent underrepresentation of women in leadership roles across Latin America. Company boards, regulators, and senior leadership teams should serve as primary owners of these initiatives.

The findings of this report make it clear that by changing industry practices, countries in Latin America can reduce the barriers women face in entering and succeeding in the cybersecurity workforce. This region is key to narrowing the workforce gap, as countries continue to develop their technology industries and can innovate as they grow. Latin American women should be given opportunities to lead and innovate in the field of cybersecurity.

Appendix A: Industry survey questions

Shaping the Future: Women's Perspectives on Cybersecurity (Industry Version)

Confidentiality Statement for Survey Participants

Your participation in this survey is completely voluntary, and your responses will be kept strictly confidential. The survey is expected to take approximately 20 minutes to complete. All information you provide will be used solely for research purposes, specifically to help inform and enhance initiatives supporting women in cybersecurity in Latin America. Individual responses will be anonymized, and no personally identifiable information will be linked to the findings. The data collected will be aggregated, and only summary results will be reported, ensuring that individual responses cannot be traced to participants. Access to the data will be restricted to authorized members of Duke University's research team, stored in accordance with data protection standards.

By participating, you agree to the collection and analysis of your responses under these terms. If you have questions about confidentiality or how your data will be used, please feel free to contact us. We appreciate your time and insights in contributing to this important research.

1. What is your gender?

- Female
- Male

2. Are you a woman working in cybersecurity?

- Yes
- No

3. What is your race or ethnicity? (Please select all that apply)

- Indigenous
- Afro-descendant
- European descendant
- Mestizo (Mixed Indigenous and European ancestry)
- Asian descendant
- Middle Eastern descendant
- Other (please specify)
- Prefer not to say

4. In which Latin American country are you currently employed?

- Argentina
- Brazil
- Chile
- Colombia
- Costa Rica
- Dominican Republic
- Mexico
- Panama
- Paraguay
- Other (please specify)

5. What is your current position level in cybersecurity?

- Entry-level
- Mid-level
- Senior-level
- Management
- Executive (C-suite)

Questions for Women in the Field

Section 1:
Entry to the Cybersecurity Field and Upskilling

6. Field of work- In which industry does your organization primarily operate?

- Government
- Non-Governmental Organization (NGO)
- Technology
- Finance
- Healthcare
- Energy
- Telecommunications
- Education
- Consumer Goods
- Materials & Industrials
- Real Estate
- Transportation
- Private Sector
- Other (please specify)

7. How many years of experience do you have in the cybersecurity field?

- Less than 1 year
- 1-3 years
- 4-6 years
- 7-10 years
- More than 10 years

8. How did you enter the cybersecurity profession?

- Traditional (STEM education)
- Non-traditional (self-taught, career transition, bootcamp, etc.)

9. For those who transitioned into cybersecurity from another field, what skill gaps did you face during your transition? (Please select all that apply)

- Lack of hands-on cybersecurity experience
- Difficulty obtaining industry-recognized certifications
- Limited access to cybersecurity-specific technical training
- Lack of clear career transition pathways
- Difficulty networking with cybersecurity professionals
- Other (please specify)
- N/A

10. What is your employment status?

- Full-time
- Part-time
- Unemployed

11. Are most of your colleagues from traditional STEM backgrounds?

- Yes
- No
- Unsure

12. Can you describe your current role and a typical workday or week?

13. What education or certifications have contributed to your hiring and career growth?

Section 2:
Workplace Environment and Inclusion

14. How would you describe the overall representation of women in your country's cybersecurity workforce?

- Very underrepresented
- Slightly underrepresented
- Balanced
- Slightly overrepresented
- Very overrepresented

15. In your organization, what percentage of cybersecurity roles are occupied by women?

- 0-10%
- 11-25%
- 26-50%
- 51-75%
- 76-100%
- I don't know

16. In your experience, what are the most common cybersecurity roles held by women in your region? (Select all that apply)

- Security Analyst
- Network Security Engineer
- Security Consultant
- Chief Information Security Officer (CISO)
- Penetration Tester
- Other (please specify)

17. How does your organization promote women's representation and empowerment within cybersecurity roles?

- Hiring initiatives
- Mentorship programs
- Training and certifications
- There are no specific initiatives
- Other (please specify)

Section 3:
Challenges and Barriers in the field

18. What are the biggest challenges women face when entering the cybersecurity field in your region? (Select all that apply)

- Lack of access to education and training
- Limited job opportunities
- Gender bias in recruitment
- Family Responsibilities
- Lack of role models
- Other (please specify)

19. Have you faced any discrimination or bias in your cybersecurity career? (Select all that apply and specify where applicable)

- Gender bias in hiring
- Unequal pay compared to male colleagues
- Lack of mentorship or sponsorship due to gender
- Bias in performance evaluations or promotions
- Exclusion from key projects or leadership opportunities
- Workplace harassment or microaggressions
- No, I have not faced discrimination or bias
- Prefer not to say

20. What barriers do women in your region face in advancing to leadership roles in cybersecurity? (Select all that apply)

- Lack of mentorship
- Lack of credentials
- Limited professional networks
- Gender discrimination in the workplace
- Balancing family responsibilities with career advancement
- Other (please specify)

Section 4:
Compensation and Job Satisfaction

21. What is your approximate annual salary in your cybersecurity role? (Optional)

- Below $20,000
- $20,000–$40,000
- $40,000–$60,000
- $60,000–$80,000
- $80,000–$100,000
- Above $100,000
- Prefer not to say

22. Do you believe there is a gender pay gap in cybersecurity roles in your country?

- Yes, it is significant
- Yes, but only in certain roles or levels
- No, pay is generally equal
- Unsure

23. How comfortable are you balancing your professional and private life?

- Extremely uncomfortable
- Somewhat uncomfortable
- Neither comfortable nor uncomfortable
- Somewhat comfortable
- Extremely comfortable

24. Which factors most impact your job satisfaction in cybersecurity? (Select all that apply)

- Salary and financial benefits
- Career growth opportunities
- Work-life balance
- Company culture and inclusivity
- Job security
- Leadership support and mentorship
- Other (please specify)

25. Have you ever considered leaving the cybersecurity field?

- Yes (If yes, what were the main reasons?
- No

26. What factors would most influence your decision to stay and grow within cybersecurity? (Select all that apply)

- Opportunities for promotion and leadership
- Access and opportunities to upskilling and professional development
- Better work-life balance
- Increased salary and benefits
- More inclusive workplace culture
- Stronger mentorship and sponsorship programs
- Other (please specify)

Section 5:
Mentorship and Networking

27. Do you have a professional mentor in cybersecurity?

- Yes
- No

28. How do you network within the field? (Select all that apply)

- Conferences
- Online forums
- Industry events
- Coffee (informal) chats
- Other (please specify)

29. How important is it to you to be part of a professional network focused on women in cybersecurity?

- Not at all important
- Slightly important
- Moderately important
- Very important
- Extremely important

30. Are you a member of any professional cybersecurity networks or communities?

- Yes (If yes, which ones?)
- No

31. Would you be interested in joining a regional mentoring network for women in cybersecurity?

- Yes (If yes, click on this link to join a regional network)
- No
- Maybe

Section 6:
Future Aspirations and Industry Improvements

32. What leadership skills are most critical for women in cybersecurity to succeed in higher-level roles? (Select all that apply)

- Strategic thinking
- Technical knowledge
- Organizational budget experience
- Decision-making under pressure
- Team management
- Communication and negotiation
- Other (please specify)

33. Has your organization offered leadership development programs tailored to women in cybersecurity?

- Yes (If yes, click on this link to join a regional network)
- No
- Maybe

34. What types of leadership development opportunities would most benefit women in cybersecurity in your region?

- Mentorship programs
- Networking events
- Online forums or discussion groups
- Workshops and training sessions
- Career fairs
- Other (please specify)

35. What support mechanisms would be most effective in helping women in cybersecurity advance to senior leadership roles? (Select all that apply)

- Leadership training programs
- Formal mentorship
- Networking events
- Flexible work policies
- Other (please specify)

36. In your opinion, what are the primary benefits of increasing diversity (including gender diversity) in cybersecurity roles within your organization or industry? (Select all that apply)

- Improved innovation and creativity
- Better representation of diverse perspectives in problem-solving
- Enhanced team collaboration and communication
- Improved ability to address diverse cybersecurity challenges
- Increased trust and credibility with clients or stakeholders
- Greater talent pool and reduced skill shortages
- Higher employee satisfaction and retention
- No perceived benefits
- Other (please specify)

37. How likely do you think increasing diversity in cybersecurity teams would improve your organization's cybersecurity performance?

- Extremely unlikely
- Somewhat unlikely
- Neither likely nor unlikely
- Somewhat likely
- Extremely likely

38. In your experience, what changes do you think are necessary at an industry or policy level to increase women's participation in the cybersecurity workforce in Latin America?

Open-Ended Questions: Insights and Recommendations

39. Based on your experience, what advice would you give to young women considering a career in cybersecurity in Latin America?

40. Which programs, resources, or networks have been especially valuable to you in your cybersecurity career? (Select all that apply and specify where possible)

- Mentorship programs
- Professional cybersecurity networks (please specify)
- Online resources or training platforms (e.g., certifications, courses)
- Conferences or industry events (please specify)
- Academic institutions or programs (please specify)
- Government or NGO initiatives (please specify)
- Company-sponsored development programs
- Community groups or forums
- Other (please specify)

Appendix B: Student survey questions

Shaping the Future: Women's Perspectives on Cybersecurity (Student Version)

Confidentiality Statement for Survey Participants

Your participation in this survey is completely voluntary, and your responses will be kept strictly confidential. The survey is expected to take approximately 20 minutes to complete. All information you provide will be used solely for research purposes, specifically to help inform and enhance initiatives supporting women in cybersecurity in Latin America. Individual responses will be anonymized, and no personally identifiable information will be linked to the findings. The data collected will be aggregated, and only summary results will be reported, ensuring that no single participant's responses can be identified. Access to the data will be restricted to authorized members of Duke University's research team stored in accordance with data protection standards.

By participating, you agree to the collection and analysis of your responses under these terms. If you have questions about confidentiality or how your data will be used, please feel free to contact us. We appreciate your time and insights in contributing to this important research.

1. What is your gender?

- Female
- Male

2. Are you a student?

- Yes
- No

3. What is your race or ethnicity? (Please select all that apply)

- Indigenous
- Afro-descendant
- European descendant
- Mestizo (Mixed Indigenous and European ancestry)
- Asian descendant
- Middle Eastern descendant
- Other (please specify)
- Prefer not to say

4. In which Latin American country are you currently employed?

- Argentina
- Brazil
- Chile
- Colombia
- Costa Rica
- Dominican Republic
- Mexico
- Panama
- Paraguay
- Other (please specify)

Section 1:
Current Career and Background

5. If working, what is your current field of work?

- Technology
- Finance
- Healthcare
- Education
- Public Service/ Government
- Arts and Humanities
- Social Services
- Science and Research
- Family or elder care
- Consumer Goods
- Materials & Industrials
- Real Estate
- Transportation
- Other (please specify)
- Not Applicable

6. What is your current STEM major? (Select the option that best applies to you)

- Computer Science
- Information Technology
- Cybersecurity
- Engineering (e.g., Electrical, Mechanical, Civil, etc.)
- Mathematics
- Physics
- Biology
- Chemistry
- Data Science/ Artificial Intelligence
- Other (please specify)

7. How familiar are you with cybersecurity as a career field?

- Not familiar at all
- Slightly familiar
- Moderately familiar
- Very familiar
- Extremely familiar

8. What is your biggest knowledge gap when it comes to cybersecurity careers? (Select all that apply)

- Understanding the different career paths in cybersecurity
- Knowing what skills or certifications are required
- Where to find training programs
- How to gain hands-on experience
- The hiring process and job-market demand
- Other (please specify)

Section 2:
Interest and benefits in Cybersecurity

9. How interested are you in pursuing a career in cybersecurity?

- Very interested
- Somewhat interested
- Neutral
- Not very interested
- Not interested at all

10. What aspects of cybersecurity attract you to the field? (Select all that apply)

- High earning potential
- Job security
- Opportunity to learn new skills
- Ability to work remotely or flexibly
- Challenging and dynamic work environment
- Impact on society and contribution to safety
- Other (please specify): _____

11. In your opinion, what are the primary benefits of increasing diversity (including gender diversity) in cybersecurity roles within your organization or industry?

- Improved innovation and creativity
- Better representation of diverse perspectives in problem-solving
- Enhanced team collaboration and communication
- Improved ability to address diverse cybersecurity challenges
- Increased trust and credibility with clients or stakeholders
- Greater talent pool and reduced skill shortages
- Higher employee satisfaction and retention
- No perceived benefits
- Other (please specify)

12. Have you encountered women role models or leaders in cybersecurity who have influenced your perception of the field?

- Yes, and it positively influenced my interest in cybersecurity
- Yes, but it didn't change my interest level
- No, I have not encountered and role models in cybersecurity

Section 3:
Barriers to Entry

13. What factors currently prevent you from considering a career in cybersecurity? (Select all that apply)

- Lack of knowledge about how to get started
- Limited access to relevant training or education
- Perception that cybersecurity is a male-dominated field
- Lack of mentorship or role models in the field
- Concerns about work-life balance in cybersecurity roles
- Lack of confidence in technical skills
- Concerns about job stress or high-stakes environment
- Other (please specify)

14. Which of your current skills do you think would be most useful in a cybersecurity career? (Select all that apply)

- Problem-solving and analytical thinking
- Communication and teamwork
- Attention to detail
- Project management and organization
- Data analysis or research
- Technical skills (e.g., coding, IT)
- Other (please specify)

15. If you were to switch to a career in cybersecurity, what type of support or resources would be most helpful to you? (Select all that apply)

- Scholarships or financial aid for training programs
- Mentorship or guidance form professionals in the field
- Networking opportunities with other women in cybersecurity
- Flexible job options to balance work and personal life
- Beginner-friendly training or introductory courses
- Clear career pathways and guidance on skill requirements
- Access to job placements or internships
- Other (please specify)

Section 4: Perception of Cybersecurity as a Career Choice

16. What concerns, if any, do you have about working in cybersecurity? (Select all that apply)

- High stress or pressure in roles
- Perception of cybersecurity as highly technical or math-intensive
- Lack of clear areer progression or advancement opportunities
- Work-life balance concerns
- Fear or bias or discrimination in a male-dominated industry
- Limited understanding of the different roles available in cybersecurity
- Other (please specify)

17. What changes or improvements in the cybersecurity industry would make it more appealing to you?

- Increased visibility of women in leadership positions
- Greater emphasis on diverse perspectives and backgrounds
- More accessible, beginner-friendly training options
- Flexible work environments
- Awareness of non-technical roles within cybersecurity
- Clearer career paths for newcomers to the field
- Other (please specify)

Endnotes

1. Panhans et al. "Empowering Women to Work in Cybersecurity Is a Win-Win." BCG. September 7, 2022.
2. Global Cybersecurity Forum. "2024 Cybersecurity Workforce Report: Bridging the Workforce Shortage and Skills Gap." GCF. October 2, 2024
3. Ibid.
4. While the survey was targeted to women, some men did complete the survey.
5. Global Cybersecurity Forum. "2024 Cybersecurity Workforce Report: Bridging the Workforce Shortage and Skills Gap." GCF. October 2, 2024
6. Panhans et al., 2022.
7. Panhans et al., 2022.
8. Panhans et al., 2022.
9. Red por la Ciberseguridad. "Women in Cybersecurity." Red por la Ciberseguridad. Accessed August 24, 2025
10. WOMCY, LATAM Women in Cybersecurity. WOMCY. Accessed August 24, 2025.
11. Global STEM Women. "Hacker Girls." Global STEM Women. Accessed August 24, 2025
12. Cisco. "Chilenas Conectadas y Seguras." PDF. Accessed August 24, 2025.
13. World Economic Forum. "The Future of Jobs in Latin America and the Caribbean: Digital Skills Gap Must Close Quickly to Satisfy Evolving Employer Demands." World Economic Forum, April 22, 2025.
14. OECD (2023), Building a Skilled Cyber Security Workforce in Latin America: Insights from Chile, Colombia and Mexico, OECD Skills Studies, OECD Publishing, Paris,
15. Global Shapers Buenos Aires. "STEM UP!" World Economic Forum. Accessed August 22, 2025
16. United Nations Development Programme. (2024, March 8). The missing piece: Valuing women's unrecognized contribution to the economy. UNDP Latin America and Caribbean.
17. UN Women. (2025, June 27). In Latin America, we're not just recognizing care work – we're rebuilding economies around it. UN Women
18. United Nations Development Programme, "Coded Bias: The Underrepresentation of Women in STEM in Latin America and the Caribbean," UNDP Latin America, May 7, 2024

Endnotes

19. Girls Who Code. Girls Who Code. Accessed August 24, 2025

20. Technovation. "2023 Impact Report." Technovation. 2024

21. Red Ciberlac. RedCiberlac. Accessed August 22, 2025

22. Bloom, Nicholas, Ruobing Han, and James Liang. "Hybrid Working from Home Improves Retention without Damaging Performance." Nature. June 12, 2024

23. Statista Market Insights. "Cybersecurity – LATAM." Statista. Accessed September 11, 2025

24. Zuzunaga et al. "Un desafío pendiente: la brecha de género en tecnología en Latinoamérica." McKinsey & Company. April 30, 2025

25. Society for Human Resource Management (SHRM). "Body of Applied Skills and Knowledge (BASK)." SHRM. Accessed August 1, 2025

GLOBAL CYBERSECURITY FORUM

Duke UNIVERSITY