REAL

RED DE EXPERTOS Y ANALISTAS LATINOAMERICANOS

WICA

Women in Cybersecurity Advancement

www.real-latam.org

REAL

RED DE EXPERTOS Y ANALISTAS LATINOAMERICANOS

WOMEN IN CYBERSECURITY ADVANCEMENT

CEXCCR PROGRAM

Merging Strengths, Bridging Gaps: Women Pioneering Cybersecurity Equity

Document elaborated by the Red de Expertos y Analistas Latinoamericanos

INDEX

ABOUT REAL
RED DE EXPERTOS Y ANALISTAS LATINOAMERICANOS

MISSION

To provide professional, innovative, and personalized strategic consulting and advisory services to organizations, institutions, or states in Security, Defense, Development, and Democracy in the Latin American region.

SERVICES

CONSULTANCY
R.E.A.L. provides consulting and advisory services in democracy, development, defense, and security with integrity and quality. Innovative and customized solutions for governments and organizations.

RESEARCH AND KNOWLEDGE MANAGEMENT
R.E.A.L. researches and manages knowledge in critical areas (security, health, education, etc.), providing practical and cost-effective solutions to transform societies.

PROJECT MANAGEMENT
R.E.A.L. provides innovative and tailored solutions to critical social problems in democracy, governance, human rights, and development, protecting vulnerable populations.

POLITICAL ANALISIS
R.E.A.L. is an NGO dedicated to multidisciplinary regional analysis for hemispheric security and integrity. Our experts inform and promote inclusive solutions.

EXECUTIVE SUMMARY

WOMEN IN CYBERSECURITY ADVANCEMENT

The Women in Cybersecurity Advancement (WiCA) is a strategic initiative to promote gender diversity and collaboration in the cybersecurity landscape. It addresses the underrepresentation of women in the field while enhancing transcontinental cooperation between the United States and the Latin American region.

WiCA has two objectives: first, to empower and advance women within the cybersecurity sector, and second, to facilitate collaboration between US and Latin American cybersecurity professionals. By providing targeted training, mentorship, and networking opportunities, WiCA equips women with the skills and confidence needed to excel in cybersecurity roles, fostering their leadership and technical contributions.

Cybersecurity is a crucial foundation for safeguarding organizations and nations against escalating cyber threats. The rapid evolution of technology and cyberspace expansion have yielded advantages and challenges. WiCA addresses the underrepresentation of women in the Americas' cybersecurity sector and the shortage of skilled cybersecurity professionals by taking a holistic and inclusive approach, providing opportunities, resources, and support for women to excel in cybersecurity.

WiCA recognizes the multifaceted benefits of women's participation in cybersecurity, striving to empower women and redefine the industry's future. By uniting stakeholders, sharing best practices, and fostering a collective approach, WiCA envisions a cybersecurity landscape that is not only safer and more resilient but also more equitable and innovative.

INTRODUCTION

WOMEN IN CYBERSECURITY ADVANCEMENT

In recent years, rapid technological advancements and the widespread expansion of cyberspace have ushered in substantial benefits, but concurrently, they have given rise to an intricate web of cyber threats with far-reaching implications for society, the economy, and national security. Cybersecurity transcends the mere protection of systems and networks; it encompasses the critical aspect of upholding trust in technology and the prevailing interconnectedness of the modern world. However, it demands a proactive approach involving fortifying cyber defenses, instilling digital security awareness, and fostering collaborative efforts among various sectors and nations.

Latin America faces unique challenges due to its ongoing technological transformation, escalating levels of connectivity, and relatively unprotected technological landscape. Despite notable progress, persistent disparities in cybersecurity measures, legislative gaps, shortages in skilled personnel, and limited regional alliances continue to impede effective cybersecurity measures. A historical lack of cybersecurity awareness leaves the region vulnerable to various threats, including social engineering and cybercrime. Scarce resources allocated to cybersecurity also pose a significant hurdle in establishing robust defenses and comprehensive training. Moreover, the prevailing political instability in certain areas gives rise to state-sponsored cyber attacks, exacerbating regional governance challenges.

In response to these challenges and with the goal of fostering regional cooperation, La Red de Expertos y Analistas Latinoamericanos - R.E.A.L. - has meticulously formulated the Regional Cyber Cooperation Center of Excellence (CexCCR) Strategic Plan. This Strategic Plan adopts a comprehensive approach, offering adaptable solutions to cultivate cooperation and leadership in cyberspace while drawing from international guidelines and frameworks. As Latin American nations endeavor to define their roles in an ever-evolving and competitive landscape, strengthening cyber capabilities becomes a strategic imperative. By fostering these capabilities, countries in the region position themselves to spearhead advancements in the industry, foresee future technological shifts, mitigate potential threats, and gain a competitive edge.

The establishment of the CexCCR stands as a critical strategic initiative designed to foster such capabilities within both the public and private sectors. Drawing upon the extensive knowledge and specialized expertise to create collaborative, interdisciplinary environments. It strives to provide comprehensive and advanced solutions to mitigate the evolving cyber threats effectively.

INTRODUCTION

WOMEN IN CYBERSECURITY ADVANCEMENT

This project is designed to address two particular issues within cybersecurity: the critical shortage of talent in Latin America and gender-based inequities. The talent deficit results from multiple intertwined factors that impede the development and retention of skilled professionals. The rapid pace of technological advancements and an expanding threat landscape have heightened the demand for specialized skills, surpassing the educational system's ability to keep pace. Concurrently, attractive job opportunities abroad allure skilled professionals from the region, intensifying the shortage and leading to a talent drain. The dynamic nature of cybersecurity necessitates continuous learning, but the lack of local professional development options contributes to skill stagnation.

Another challenge exacerbating the talent shortage is the inadequate representation of women in the cybersecurity sector. Enhancing the involvement of women in cybersecurity is not merely about filling staffing gaps; it holds the promise of infusing the discipline with a broader spectrum of problem-solving approaches and innovative insights. This diversification, in turn, can enhance business efficacy, stimulate economic growth, and bolster regional security. Encouraging women to join the field and providing them with advancement opportunities are critical steps to ensure a skilled, diverse, and ample cybersecurity workforce in the years ahead.

Despite constituting nearly half of the global workforce, women comprise mainly 25% of cybersecurity professionals due to various factors, including industry perception, family constraints, limited digital literacy, wage gaps, and promotion disparities. Simultaneously, female internet users face a higher incidence of cybercrime and online harassment, leading to increased risks of financial loss and privacy breaches. This underrepresentation hampers secure economic and societal development.

Addressing these challenges is crucial for fostering a safer, more inclusive cyberspace that closes workforce and gender gaps, ultimately promoting greater equity and security, but demands collaborative efforts among academia, industry, and governments to bridge the skills gap and foster expertise in the region. The Women in Cybersecurity Advancement (WiCA) is an initiative designed to address the need for gender equity in the Americas' cybersecurity sector. Our project's significance lies in fortifying these digital foundations for women by elevating women's participation in cybersecurity beyond filling vacancies. It promises to enrich problem-solving and innovation by injecting diverse perspectives, thereby enhancing business performance and economic growth.

INTERNATIONAL FRAMEWORK

WOMEN IN CYBERSECURITY ADVANCEMENT

The United Nations, the Organization of American States, and other global organizations are actively promoting gender equality and empowering women in STEM fields, including cybersecurity. These initiatives are designed to address the overarching issue of gender disparities in the workforce and the underrepresentation of women in cybersecurity roles.

The United Nations Sustainable Development Goals (SDGs) Goal 5 focuses on achieving gender equality and empowering all women and girls. The UN Women's Empowerment Principles (WEPs) encourage businesses to adopt practices that promote gender equality in the workplace, including sectors like STEM and cybersecurity. UNESCO's STEM and Gender Advancement (SAGA) Project promotes gender equality in STEM education and careers. The International Telecommunication Union (ITU) has various initiatives to promote gender equality in the tech sector, including its Girls in ICT, which encourages girls to consider careers in information and communication technology, including cybersecurity.

The Organization of American States (OAS) promotes cooperation and dialogue among its member states, consistently supporting initiatives aimed at addressing gender disparities in the workforce and promoting women's empowerment. These efforts can indirectly impact various sectors, including cybersecurity. For example, the OAS Cybersecurity Capacity Building Efforts benefit all individuals working in the field of cybersecurity, including women. The OAS also promotes gender equality and women's empowerment in the Americas. While not specific to cybersecurity, its objectives include promoting equal access to economic opportunities for women and supporting initiatives that aim to increase women's participation in STEM fields.

Other organizations are also working to address the need for increased female representation in cybersecurity. For example, the Cybersecurity and Infrastructure Security Agency (CISA) collaborates with global organizations to bridge the gender gap by enabling women to access education, conferences, and career opportunities. CISA emphasizes the importance of STEM education and hands-on experiences, encouraging interactive learning and internships that can empower women and boost confidence in their abilities while fostering diversity and excellence within CISA's mission.

OBJECTIVES

EDUCATION, NETWORKING, EXPERIENCE

To address the challenges of gender inequality in cybersecurity, a comprehensive strategy is essential. This project focuses on empowering women throughout their cybersecurity careers, **from education to employment to advancement**. It requires the involvement of all stakeholders, including governments, corporations, educational institutions, NGOs, and individuals. By working together, we can foster collective action and share best practices to bridge the gender gap, bolster industry innovation, and amplify cyber resilience. Recognizing diversity as a strategic asset, this project aligns with global security resolutions, propelling cybersecurity into a more inclusive and forward-looking realm in line with the Women, Peace, and Security agenda.

1

EDUCATION AND TRAINING ENHANCEMENT

Create a customized cybersecurity educational program designed to cater specifically to the requirements of women. This objective seeks to provide women with the skills and knowledge they need to succeed in cybersecurity careers. This program should be designed in consultation with women in cybersecurity to ensure that it is relevant to the needs and interests of the participants and the industry. It should be inclusive of all women and regularly updated to reflect the latest trends and developments in cybersecurity.

MENTORSHIP AND NETWORKING

2

Establish a robust community for women in the cybersecurity sector to empower women to thrive in the industry. This objective involves implementing a mentorship initiative to connect aspiring female professionals with experienced counterparts. This allows access to networking, advice, and career perspectives from role models who have overcome the challenges prevalent in cybersecurity. It should celebrate the achievements of women, recognizing their contributions to the field.

3

HANDS-ON EXPERIENCE

Bridge the gap between theoretical knowledge and practical skills. This objective will collaborate with cybersecurity firms and organizations to provide internships, apprenticeships, and project-based learning opportunities. These experiences will give women real-world experience, insights into the industry, and the opportunity to apply their skills to actual cybersecurity challenges, enhancing their practical competencies and confidence in the field. This will promote a more representative and better equipped workforce.

ACTIVITIES

EDUCATION AND TRAINING ENHANCEMENT

Phase/Stage: Initial phase

Description: A focused and customized cybersecurity educational program tailored to meet women's unique needs and requirements in the field. The program aims to provide knowledge, skills, and support to help women succeed and thrive in cybersecurity.

Scope & Timeline: Q1 & Q2 Organized learning modules and practical exercises, it will be a comprehensive yet condensed curriculum, allowing for in-depth learning while remaining achievable within the specified timeframe.

Target Audience: Women who are interested in pursuing careers in cybersecurity. Women who are already working in cybersecurity but want to advance their skills. Organizations that are committed to diversity and inclusion in the workplace.

Proposed Learning Plan Modules:

- **Introduction to Cybersecurity:** Understand the fundamentals of cybersecurity and recognize the importance of diversity and inclusion in the cybersecurity field.
- **Cyber Threats and Attacks:** Identify common cybersecurity threats and attack vectors and understand the impact of cyber threats on organizations and individuals.
- **Cybersecurity Technologies:** Familiarize with key cybersecurity technologies and tools and learn about firewalls, encryption, intrusion detection systems, etc.
- **Secure Coding and Software Development:** learn about application security and common vulnerabilities.
- **Compliance and Legal Aspects:** Understand legal and compliance requirements in cybersecurity and learn about privacy laws, data protection regulations, and ethical considerations.
- **Career Development and Networking:** Develop skills for career growth in the cybersecurity sector and learn effective networking strategies and personal branding techniques.

At the end of each module, participants will undergo assessments or submit project work related to the module's content. The program will culminate in a comprehensive evaluation based on module assessments, participation, and project completion, contributing to the overall program completion rate and participant satisfaction.

ACTIVITIES

EDUCATION AND TRAINING ENHANCEMENT

Expected Outcomes:

- Increased interest in cybersecurity careers among women: The gamified learning platform, cybersecurity virtual labs, and specialized cybersecurity curriculum are all designed to be engaging and relevant to women. This could lead to more women considering cybersecurity as a career option.
- Improved skills and knowledge of women in cybersecurity: The training programs and scholarships offered specifically for women will give them the skills and knowledge they need to succeed in this field. This could lead to more women entering and advancing in cybersecurity careers.
- A more diverse and inclusive cybersecurity workforce: The activities described above are all designed to make cybersecurity more accessible and welcoming to women. This could lead to a more diverse and inclusive cybersecurity workforce, which is essential for protecting our critical infrastructure and sensitive data.

Promotion Strategy: The curriculum and different activities involved will be offered online and will be promoted through a variety of channels, including social media, conferences, and outreach programs. The curriculum could be evaluated on a regular basis to ensure that it is meeting the needs of women in cybersecurity.

ACTIVITIES

MENTORSHIP AND NETWORKING

Phase/Stage: Initial phase and throughout the entire project.

Description: Launch a regional cybersecurity mentorship program to pair aspiring women in cybersecurity with experienced professionals. This program will allow women to get one-on-one advice and guidance from successful women in the field. We will also launch a public awareness campaign to promote cybersecurity as a career option for women.

This activity will be structured as follows:

- Each mentee will be paired with a mentor with experience in their desired field of cybersecurity.
- The mentor and mentee will meet regularly to discuss the mentee's career goals, provide guidance, and answer questions.
- The program will also include an online community where mentees can connect with other women in cybersecurity, ask questions, share experiences, and get support.

This program aims to help aspiring women in cybersecurity achieve their career goals. By providing them with access to experienced professionals and a supportive community, we can help them build the skills and confidence they need to succeed in this field.

Timeline: Q1, Q2, Q3 and Q4.

Target Audience: Women who are interested in pursuing careers in cybersecurity. Women who are already working in cybersecurity but want to advance their skills. Organizations that are committed to diversity and inclusion in the workplace.

Expected Outcomes:

- Increased confidence and motivation: The mentorship program will allow women to learn from successful women in the field, which can help boost their confidence and motivation. This could lead to more women pursuing careers in cybersecurity.
- Improved skills and knowledge: The mentorship program will provide women with access to the knowledge and skills they need to succeed in cybersecurity. This could lead to more women entering and advancing in cybersecurity careers.
- A more diverse and inclusive cybersecurity workforce: The mentorship program will create a space where women can connect with other women in the field and build relationships. This could lead to a more diverse and inclusive cybersecurity workforce, which is essential for protecting our critical infrastructure and sensitive data.

ACTIVITIES

HANDS-ON EXPERIENCE

Phase/Stage: Final phase.

Description: This objective seeks to bridge the gap between theoretical knowledge and practical skills by collaborating with cybersecurity firms and organizations. Internship and apprenticeship opportunities will be established, allowing women to gain real-world experience and insights into the workings of the industry. Additionally, remote project-based learning experiences will be offered, enabling participants to apply their skills to actual cybersecurity challenges, enhancing their practical competencies and confidence in the field.

- Capture The Flag (CTF) Competitions: A series of CTF competitions exclusively for women, ranging in difficulty levels. Grants can be used to create engaging challenges, provide attractive prizes, and ensure that competitions are well-publicized. This approach encourages healthy competition, skill-building, and community interaction.
- Cybersecurity Innovation Hackathons: These focus on addressing specific cybersecurity challenges various sectors face. Participants can work in diverse teams to develop innovative solutions, fostering collaboration and problem-solving skills. Grants can cover event costs, mentorship resources, and the development of prototypes emerging from these hackathons.
- Partner with cybersecurity firms and organizations to offer internship and apprenticeship opportunities for women. This will give women the opportunity to gain real-world experience in the field and learn from experienced professionals.

Timeline: Q3 and Q4.

Target Audience: Women who are interested in pursuing careers in cybersecurity. Women who are already working in cybersecurity but want to advance their skills. Organizations and companies that are committed to diversity and inclusion in the workplace.

Expected Outcomes:

- **Increased practical skills:** Women will gain real-world experience in cybersecurity through internships, apprenticeships, and remote project-based learning experiences. This will enhance their practical skills and confidence in the field.
- **Improved understanding of the industry:** Women will gain insights into the workings of the cybersecurity industry through their interactions with professionals and their participation in CTF competitions and hackathons. This will help them to better understand the skills and knowledge they need to succeed in this field.
- **A more diverse and inclusive cybersecurity workforce:** The increased participation of women in cybersecurity will lead to a more diverse and inclusive workforce. This is essential for protecting our critical infrastructure and sensitive data.

ALLIANCE PARTNERSHIP

CORPORATE PARTNERSHIPS

CyberTech | US$5,000/year

Private and public companies, technology vendors

Benefits

- R.E.A.L. Corporate Partner badge
- Newsletter recipient (email)
- Members-only access website
- Quarterly Program Execution report
- All-Hands quarterly invitation & recording
- R.E.A.L. Talent: Corporate profile / Job board posting / Resume access
- Sponsored video or article introducing partner in our channels (YouTube or blog)
- Partner Sponsored Webinar, hosted & organized by R.E.A.L. (2 per year)
- R.E.A.L. Blog article (4 per year)
- Speaking engagement at partner's event (2 per year)
- Promotional material to members
- Mentoring participation

Branding and Marketing

- Partner Logo included in website
- Partner Logo included in presentations and events
- Partner Logo included in newsletter
- Partner promotional material at events
- Joint Press Release
- Social media profile promotion (4 per year)

ALLIANCE PARTNERSHIP

CORPORATE PARTNERSHIPS

CyberCorp | US$2,500/year

Private and public companies, technology vendors.

Benefits

- R.E.A.L. Corporate Partner badge
- Newsletter recipient (email)
- Members-only access website
- Quarterly Program Execution report
- All-Hands quarterly invitation & recording
- R.E.A.L. Talent: Corporate profile / Job board posting / Resume access
- Sponsored video or article introducing partner in our channels (YouTube or blog)
- Partner Sponsored Webinar, hosted & organized by R.E.A.L. (1 per year)
- R.E.A.L. Blog article (2 per year)
- Speaking engagement at partner's event (1 per year)
- Promotional material to members
- Mentoring participation

Branding and Marketing

- Partner Logo included in website
- Partner Logo included in presentations and events
- Partner Logo included in newsletter
- Partner promotional material at events
- Joint Press Release
- Social media profile promotion (2 per year)

ALLIANCE PARTNERSHIP

CORPORATE PARTNERSHIPS

CyberBiz | US$1,000/year

Private and public companies, technology vendors.

Benefits

- R.E.A.L. Corporate Partner badge
- Newsletter recipient (email)
- Members-only access website
- Quarterly Program Execution report
- All-Hands quarterly invitation & recording
- R.E.A.L. Talent: Corporate profile / Job board posting / Resume access
- Sponsored video or article introducing partner in our channels (YouTube or blog)
- R.E.A.L. Blog article (1 per year)

Branding and Marketing

- Partner Logo included in website
- Partner Logo included in presentations and events
- Partner Logo included in newsletter
- Partner promotional material at events
- Joint Press Release
- Social media profile promotion (2 per year)

ALLIANCE PARTNERSHIP

STRATEGIC SUPPORTERS

CyberDonation

1. Educational Institutions, Universities, Schools, Training and Certification Centers.
2. Government entities, foundations, non-profit organizations.
3. Communication Channels, Magazines, Publications, Radio, Digital Media.

Benefits

- Partner Logo included in R.E.A.L. website
- Partner Logo included in WOMCY presentations and events
- Partner Logo included in WOMCY newsletter