WEAVING DIGITAL SECURITY

COMMUNITY DIGITAL GUARDIANS: A TRAINING OF TRAINERS CURRICULUM ON CYBERSECURITY, GOVERNANCE, AND DIGITAL RIGHTS FOR INDIGENOUS AND AFRO-DESCENDANT ORGANIZATIONS, COMMUNITIES, AND PEOPLES IN COLOMBIA

September 2025

DATA GOYÁ INSTITUTE

Community Digital Guardians: A Training of Trainers Curriculum in Cybersecurity, Governance, and Digital Rights for Indigenous and Afro-descendant Communities in Colombia / Authored by Umut Pajaro Velásquez, Denise Machado Leal, and Jose A. Rojas Marcelo; Content by Umut Pajaro Velásquez; Ethnic Perspective Review by Saya Pasillo; Edited and Styled by Denise Machado Leal. -- Rubiataba, Goiás, Brazil : Instituto Data Goyá, 2025. 43 p.

Includes references.
Original Text in Spanish.
Version in English.

Work Identification Number: 032025 - Version of September 29, 2025

1. Digital Education - Colombia - Curricula. 2. Cybersecurity - Study and Teaching - Colombia. 3. Indigenous Peoples - Education - Colombia. 4. Afrodescendants - Education - Colombia. 5. Training of Trainers.

CDD 370

Contact information:
Rubiataba, Goiás, Brazil.
Email: denise@datagoya.com.br

More resources available at https://datagoya.com.br/

Authors
Umut Pajaro Velásquez
Denise Machado Leal
Jose A. Rojas Marcelo

Content
Umut Pajaro Velásquez

Ethnic Perspective Review
Saya Pastillo

Style, Design and Editing Review
Denise Machado Leal

Weaving Digital Security Project Work Team:
Denise Machado Leal – Leader, Data Protection Expert for Indigenous and Traditional Peoples, and Training of Trainers Designer
Umut Pajaro Velásquez – Co-leader, Expert in Internet Governance and Digital Education, and Curriculum Designer
Jose A. Rojas Marcelo (Quantvia Legal Advisors) – Co-leader, Digital Security Expert, and Digital Security Assessment Designer
Ximena Cuzcano – Expert in Digital Security and Gender Perspective
Saya Pastillo – Expert in Technology and Internet Governance from the Perspective of Indigenous Communities and Peoples
Karen Gutiérrez – Expert Integrator of Communities, Peoples and Local Organizations (Colombia)
Isac Pulido – Intern and Support in Integration and Communication Processes.

COMMUNITY DIGITAL GUARDIANS: A TRAINING OF TRAINERS CURRICULUM ON CYBERSECURITY, GOVERNANCE, AND DIGITAL RIGHTS FOR INDIGENOUS AND AFRO-DESCENDANT COMMUNITIES IN COLOMBIA

In collaboration with HIVOS, within the framework of the “Connect, Defend, Act” project in Colombia, the Data Goyá Institute and its team developed this digital security curriculum tailored to Civil Society Organizations (CSOs), which includes the following topics: Introduction to digital security, studies on data protection legislation and regulations applicable to CSOs, Identification of and response to the most common cyberthreats faced by CSOs, Encryption tools and secure communication, and Risk mitigation strategies.

In addition, we have collaborated with the Community Action facilitator organization designated by HIVOS (SIDOC Foundation) and other organizations to provide suggestions, feedback, reflections, and content design for an effective curriculum that ensures an adequate response to the needs of CSOs. The curriculum includes clear assessment methods that guarantee its effectiveness and measurability, and ultimately results in sustainable digital security training. We thank HIVOS for the collaboration and opportunity.

SUMMARY

1. INTRODUCTION: FUNDAMENTALS FOR THE TRAINER OF TRAINERS

This curriculum is intended as a tool to strengthen the capacities of Indigenous and Afro-descendant leaders in Colombia, who will assume the role of community trainers in digital security. Its purpose is to offer a conceptual and methodological foundation that combines Training of Trainers (TOT) with Popular Education, ensuring participatory, culturally relevant, and action-oriented learning processes.

Future Digital Guardians will not only receive technical knowledge but will also develop pedagogical and organizational skills to replicate the learning process in their communities. In this way, the training goes beyond the simple transmission of information and becomes a collective process of empowerment, capable of addressing the gaps in access, ownership, and digital security that these territories face.

In this sense, the curriculum is based on three main foundations: recognizing technology as a space that can reproduce inequalities or strengthen community autonomy; promoting a dialogue of knowledge, linking technical knowledge with ancestral and organizational knowledge; and ensuring that each module leads to concrete actions that strengthen community technological sovereignty and the defense of rights in the digital environment.

1.1 PURPOSE AND PHILOSOPHY OF THE CURRICULUM

This document presents a curriculum proposal designed to train leaders from Indigenous and Afro-descendant communities in Colombia, with the goal of becoming "Digital Guardians." This is not a traditional technical manual, but rather a political and pedagogical proposal. Its fundamental purpose is to empower these communities so that they not only use digital technologies safely, but also actively participate in building a more just, equitable, and inclusive internet ecosystem. Digital Guardians will be facilitators capable of protecting their communities, defending their collective and individual rights in the digital environment, and articulating their voices in the spaces where the future of the internet is decided.

The philosophy underlying this curriculum is based on the recognition that technology is not a neutral tool. Its design, implementation, and governance can both replicate and amplify existing power structures and inequalities, as well as challenge them. [1] Therefore, technological appropriation must be a critical, conscious, and collective act, aimed at

strengthening the autonomy and life plans of each community.

1.2 THE PEDAGOGICAL APPROACH: HYBRIDIZING THE TRAINING OF TRAINERS WITH POPULAR EDUCATION

To achieve a profound and sustainable impact, this curriculum merges two powerful pedagogical approaches: Training of Trainers (TBT) and Popular Education (PE).

1.2.1 Principles of Training of Trainers (TOT)

The FdF model provides the structure for effectively scaling knowledge. It is organized into a three-stage process: a pre-training phase to identify needs, an intensive training phase, and a post-training phase to support replication. [2] The objective of the FdF is not simply to transfer information, but rather to "develop students," [3] empowering them in crucial skills such as planning training actions, designing teaching materials, and evaluating processes. [4] New trainers are expected to develop autonomy and creativity, aspiring not to imitate the teacher, but to "seek what they seek," that is, to find their own solutions to the challenges in their environment. [3]

1.2.2 Principles of Popular Education (EP) and the Dialogue of Knowledge

A standard FdF model is insufficient for such specific cultural and political contexts. Therefore, it is enriched with PE principles, ensuring its cultural relevance and empowering potential.

- Starting from Reality: Every educational process must begin with a critical analysis of the participants' own reality. [6] Their experiences, knowledge, and struggles are not an anecdotal starting point, but a legitimate source of knowledge that structures all learning.
- Knowledge Dialogue: The traditional hierarchy between the "expert" who teaches and the "apprentice" who receives is broken. The facilitator's technical knowledge enters into a horizontal dialogue with the community's ancestral, organizational, territorial, and cultural knowledge. [8] Knowledge is co-constructed collectively, recognizing that each participant is a bearer of valuable knowledge.
- Praxis (Action-Reflection-Action): Learning is a dynamic cycle that continues in the classroom. Each module is designed to lead to a specific action within

the community. Reflection on the results of that action feeds into and enriches the next learning cycle, ensuring that knowledge is applied and transformed into experience ·

- Political Dimension: Education is an inherently political act. This curriculum does not seek to develop passive consumers of technology, but rather critical individuals, aware of the power relations in the digital environment and capable of organizing themselves to transform their realities ·

1.3 CONTEXT: THE DIGITAL REALITY OF ETHNIC COMMUNITIES IN COLOMBIA

The development of this curriculum responds to the complex and paradoxical context that Indigenous and Afro-descendant communities in Colombia face in their relationship with the digital world.

- **The Persistent Access Gap:** On the one hand, there are important government and private sector initiatives to expand connectivity. Programs such as "Internet Boards," "Connectivity to Change Lives," and the deployment of 4G infrastructure seek to connect millions of Colombians in rural and remote areas. [11] However, the reality in many territories is different. Research in departments such as Vaupés reveals access "by the dropper": intermittent, with very low speeds, and often limited to small community connection points, which prevents meaningful use of the network. [13] The gap in internet coverage between Indigenous and non-Indigenous households remains a palpable reality. [1]
- **The Digital Proficiency Gap:** Access to infrastructure is only part of the challenge. The digital divide has multiple facets: motivational (the desire to connect), material (access to devices and affordability), skills, and usage (the ability to leverage the connection for relevant purposes). [13] A report by the Karisma Foundation reveals that 72% of human rights defenders in Colombia, many of them belonging to ethnic communities, have low or medium levels of digital proficiency, which directly increases their vulnerability. [15] The lack of adequate support and culturally relevant content can turn simple access into a new risk. [14]
- **A Complex Risk Ecosystem:** The arrival of connectivity, in the absence of adequate preparation, exposes communities to a diverse ecosystem of risks. These range from the exposure of children and adolescents to inappropriate content such as violence or pornography [16] , to the erosion of cultural identity due to the influence of global lifestyles that may seem more attractive to youth. [14] Even more serious, the digital space has become a new front of attack against social, environmental, and community leaders. Direct threats, cyberbullying, smear campaigns, phishing (impersonation to steal information), and

unauthorized access to accounts are commonly reported incidents. [15]

Colombian public policy has promoted connectivity as a fundamental solution for development and closing gaps. [12] Official discourse has focused on expanding physical infrastructure and increasing the number of connections. However, evidence from civil society organizations and academic research shows that this access, when it finally reaches the most remote territories, is often precarious and not accompanied by training processes that respond to local needs and realities. [13]

This disconnect between infrastructure policy and the reality of appropriation creates a profound paradox: connectivity, presented as a tool for empowerment, can become a vector of new and serious sociocultural and security risks. [14] Communities are immersed in a digital environment designed in other contexts, with market logic and values that may be alien or even contrary to their worldviews and forms of organization. [17] The challenge, therefore, is not simply the "lack of internet," but the lack of an internet that belongs to them and serves them.

Consequently, this curriculum aims to go beyond traditional “digital literacy,” which is limited to teaching the use of tools. The goal is to move toward building **“Community Technological Sovereignty** .” This concept implies that communities develop the collective capacity not only to use technology safely, but also to govern it: to decide *which* technologies to adopt, *how* to integrate them according to their own values and life plans, and *for what* purposes to use them, such as strengthening their autonomy, defending their territories, and promoting their cultures. The curriculum thus becomes a tool for building this sovereignty from the ground up.

2- MODULES

The curriculum is structured into six progressive modules that combine theory, practice, and collective reflection, designed to respond to the needs of Indigenous and Afro-descendant communities in the face of the challenges of the digital world.

Module 1 introduces the notion of digital territory, explaining in an accessible way what the Internet is, who its main actors are, and how information circulates. It also includes practical activities that connect technology to local reality. Module 2 addresses rights

in the digital world, showing how human rights are expressed online, how to defend them, and what legal and community tools can be used.

Module 3 focuses on community cybersecurity, providing basic knowledge of digital care, risk mapping, and a catalog of free and secure tools, reinforcing the idea of collective care. Module 4 explores internet governance and community participation, linking local struggles with national, regional, and global scenarios, and promoting the development of community-based agendas.

Module 5 develops incident response protocols, offering clear guidelines and practical exercises so communities can react in an organized and effective manner to digital threats. Finally, Module 6 focuses on the role of the community trainer, offering pedagogical, methodological, and planning tools to ensure the curriculum is replicated in each territory, consolidating a multiplier effect.

Together, these modules guarantee a comprehensive training process that articulates technical learning with the political, cultural, and organizational strengthening of communities on their path toward digital sovereignty.

2.1 MODULE 1: OUR DIGITAL TERRITORY - UNDERSTANDING THE INTERNET ECOSYSTEM

The goal is to demystify technology and build a fundamental and critical understanding of how the Internet works, who its key players are, and how it relates to physical and community environments.

2.1.1 What is the Internet? From the Abstract to the Concrete (Pedagogy of Analogy)

For a meaningful understanding of the Internet, it is crucial to anchor it in concepts and realities familiar to communities. The network's physical infrastructure, submarine cables, fiber optics, satellites, and antennas, will be explained using analogies with elements of the territory, such as the rivers that connect communities, rural paths, or oral communication networks that weave the social fabric. The connectivity efforts of the Ministry of Information and Communications Technology (MinTIC)[11] will be visualized on maps of the country, showing the locations of the "main roads" of information and where digital "traffic lanes" or "zones of silence" persist, often coinciding with ethnic territories.

Practical Activity: Mapping Our Digital Territory

On a physical map of the reservation, community council, or collective territory, participants will draw their connection reality. They will identify where they connect (at home, at a kiosk, in the park), who provides that connection (a company, a community Internet Board), the type of access (WiFi, mobile data), and map the signal quality in different areas. They will also discuss the associated economic costs, a key factor limiting access for many families. [1] This activity transforms the abstract concept of "the network" into a tangible, economic, and geographic reality, allowing for an initial collective assessment of their connection strengths and weaknesses. [13]

2.1.2 Who Rules the Internet? Actors and Power in the Digital Ecosystem

The Internet is not an ungoverned space; its rules and direction are the result of interaction, and often tension, between various actors. The multi-actor (or *multi-stakeholder*) model that defines Internet governance will be presented, comprising the government, the private sector, academia, civil society, and the technical community. [The] most relevant actors in the Colombian context will be identified, explaining their roles and interests:

- **Government:** Ministry of ICT and the Communications Regulation Commission (CRC), responsible for formulating public policies and regulating the sector
- **Private Sector: Companies such as Google, Telefónica, and local internet providers, whose main** [focus] is expanding services and maintaining infrastructure.
- **Civil Society:** Organizations such as the Karisma Foundation, the Foundation for Press Freedom (FLIP), and Colnodo, which advocate for an internet with a social and human rights focus
- **Academia:** Universities that research the social and cultural impacts of technologies. [19]

Practical Activity: Role Play: The Governance Table

To help participants understand power dynamics firsthand, a role-play will be conducted. They will be assigned to represent the different actors and a relevant discussion topic will be presented, such as: "A telecommunications company wants to install an antenna at a community sacred site in exchange for providing free internet." Each group will defend

the interests of their role. The objective is for them to experience the tensions, negotiations, and power imbalances that exist in decision-making about the future of the internet, understanding why it is crucial for their own voice to be present in these discussions .

2.1.3 The Flow of Information: Where Does It Come From and Where Does It Go?

Basic technical concepts will be explained in an accessible way, again using analogies. Servers and the cloud can be compared to a community garden where information is planted and stored. IP addresses are like the address of a house, and data packets are like the letters that a messenger carries from one place to another. A critical aspect of the current internet will be addressed: the centralization of information and services in a handful of large technology corporations. [21] This has direct implications for cultural diversity, information control, and data sovereignty.

Practical Activity: The Path of a Message

Participants will trace the hypothetical journey of a WhatsApp message or photo sent from their community to a family member in another city. They will identify all the intermediaries that "touch" or can "see" that message: the local internet provider, fiber optic cables, Meta servers (Facebook/WhatsApp) in other countries. This visual and practical exercise provides an intuitive understanding of the vulnerability of information and lays the groundwork for understanding the vital importance of encryption, which will be addressed in Module 3.

For Indigenous and Afro-descendant communities, the concept of “territory” transcends the purely physical; it is a complex network of social, cultural, spiritual, and self-governing relationships. The arrival of digital technology not only introduces a tool but also creates a new space for interaction that can be understood as an extension of their ancestral territory: the **digital territory** . [13] This new territory is not a neutral space. It is shaped and governed by actors with economic and political interests that are often alien to or even contrary to those of the communities. [19] The same historical struggles over land, autonomy, and the protection of natural resources are replicated and take on new forms in this domain. The dispute over the radio spectrum, the defense against the mass extraction of personal data (the new extractivism), and the fight for a dignified and non-folklorized cultural representation are examples of these tensions.

Therefore, this module must frame the understanding of the Internet not as an external tool to be "used," but as a new territory to be governed, defended, and appropriated according to the principles of territorial governance. This redefinition is fundamental for culturally relevant and politically mobilizing appropriation. Concepts such as "cybersecurity" can be translated into the practice of "digital indigenous guardianship," and "internet governance" becomes the task of building a "digital life plan" that articulates with the community's life plan.

2.2 MODULE 2: OUR RIGHTS IN THE DIGITAL WORLD

The goal is to translate the abstract framework of digital rights into concrete and defensible situations, empowering participants to recognize violations and demand guarantees from both platforms and the State.

2.2.1 From Human Rights to Digital Rights: A Natural Extension

A fundamental principle will be established: digital rights are not a new and separate category of rights. They are the extension and application of universally recognized human rights—such as the right to privacy, freedom of expression, non-discrimination, or access to information—to the digital environment. [22] The Colombian legal framework will be reviewed, which has a solid foundation such as Law 1581 of 2012 on the Protection of Personal Data and a rich body of jurisprudence from the Constitutional Court that has adapted these rights to the online world. [24]

Practical Activity: Word Circle: What Rights Are Important to Us?

Learning will begin within the community itself. A dialogue (speaking circle or online forum) will be opened where participants will share the rights and values most relevant to their worldview and daily struggles: the right to autonomy, prior consultation, one's own culture, and the right to land and territory. From this foundation, a collective reflection will be guided on how the advent of technology (a cell phone, an internet connection) is affecting, strengthening, or jeopardizing these fundamental rights.

2.2.2 “Translating” Rights: From Law to Everyday Life

To be useful tools, rights must be understandable and applicable. This submodule will focus on "translating" each key right into simple language and everyday situations.

- **Right to Privacy and Data Protection** [23] : The right to decide what is shared about oneself, one's family, and one's community will be explained. The concept of informed consent will be analyzed: Do we really understand what we are giving permission to when we install an app? The case of the CoronApp application, promoted by the government during the pandemic, will be used as an example of mass data collection and the debates it generated about privacy. [27]
- **Right to Freedom of Expression** [23] : Its limits and scope will be explored. What can I say online? The crucial difference between critical opinion, verifiable information, and hate speech or incitement to violence will be addressed. The issue of content moderation will be analyzed, where decisions by foreign technology companies can silence legitimate voices, as happened with complaints during the 2021 National Strike .
- **Right to be Forgotten** [23] : It will be presented as the right to request the removal from the internet of personal information that is false, no longer relevant, or causes unjustified damage to a person's reputation.
- **Right to Cultural Identity and Anonymity:** The duality of digital identity will be discussed: it can be a tool to strengthen and disseminate one's culture, but also a risk of folklorization or weakening community identity, especially among young people. [14] The right to anonymity will be addressed as an essential protection tool for defenders and activists facing persecution. [25]
- **Protection of Children and Adolescents (NNA): The risks that children and adolescents face online (exposure to harmful content, cyberbullying, grooming) and the responsibilities of families and communities in supporting and protecting them will be** specifically addressed, in line with Colombian legislation that seeks to create safe digital environments for them.

2.2.3 Defending Our Rights: Mechanisms and Allies

Recognizing a violated right is the first step; knowing how to defend it is what empowers. Practical avenues for enforcing rights will be explained:

- **Platform Mechanisms:** How to use content reporting tools on networks like Facebook or YouTube.
- **Action for Protection:** The legal mechanism for protecting fundamental rights will be explained, but its current limitations will also be pointed out, since the Constitutional Court has determined that, in many cases, the claim process with

the platform must be exhausted first, which can generate delays and uncertainty .

- **Partner Organizations:** The role of civil society organizations that are key allies in the defense of digital rights in Colombia will be presented, such as FLIP , Dejusticia , and **Access Now** , which can offer legal and technical advice.

Practical Activity: Complaint Simulation

In small groups, participants will work through a hypothetical case relevant to their context (e.g., "A tourism company posts photos of a sacred ritual on Instagram without the community's permission, using them for advertising"). They will design a step-by-step strategy to request the content's removal, detailing what they would do first (report to the platform), what information they would gather, and which ally they could contact if the platform doesn't respond.

2.2.4 Digital Rights Translation Matrix

The following table serves as the central pedagogical tool for the module. Its objective is to translate abstract legal concepts into a practical and actionable format, directly connected to reality and community values.

Digital Law (Formal Language)	**What Does It Mean in Our Community? (Translation)**	**Risk/Violation Example**	**How Do We Defend It? (Community Action)**
Right to Privacy and Protection of Personal Data (Law 1581) [24]	The right to decide who can know things about us, our family, and our community. It's like deciding who we invite into our maloca or home.	A government health app requests access to all my contacts and photos without explaining why. [27] Photos of a community leader are posted on social media with false information to threaten him. [15]	1. Don't give the app permission. 2. Ask the community if others are having the same problem. 3. Contact a partner organization for advice. 4. Use encrypted messaging to discuss the issue.
Right to Freedom of Expression [23]	The right to tell our truth, to denounce injustice, and to share our ideas, as long as	Facebook removes a video where the Indigenous guard is documenting	1. Save a copy of the video. 2. Appeal the decision on the platform. 3. Document the case

	we don't call for violence against others. That's our word on the internet.	abuse, saying it is "violent content. "	(screenshots). 4. Contact FLIP or a partner media outlet to expose the censorship.
Right to Identity and Own Culture [14]	The right to have our culture, language, and traditions respected on the internet, and to decide how we want to show them to the world, without being turned into an ornament.	An influencer visits the community, films the children without their parents' permission, and uploads a video mocking their customs.	1. Report the video to the platform for harassment or disrespect toward minors. 2. Organize a community response on social media, explaining why the content is harmful. 3. Create your own content that showcases culture with dignity.
Right to Protection of Children and Adolescents on the Internet [16]	The entire community has a duty to protect our young people so they can enjoy the internet safely, protecting them from deception and abuse.	An unknown adult contacts a young woman in the community through social media, asks for intimate photos, and then threatens to publish them if she doesn't give him money (sextortion).	1. Support the young woman, assuring her that it's not her fault. 2. Don't give in to extortion. 3. Block and report the abuser. 4. Document the threats. 5. Seek support from specialized organizations or the ICBF.

For ethnic communities in Colombia, whose history is marked by the struggle for territorial rights and autonomy, the defense of their rights in the digital environment takes on a strategic dimension. Threats to their physical and cultural survival often begin with stigmatization, misinformation, and attacks against their leaders and organizational processes. [22] Today, a significant portion of this violence is perpetrated in the digital space. [15] Smear campaigns on social media, the impersonation of their organizations, or the digital surveillance of their communications are not isolated technological problems; they are the new weapons used in the dispute over territory.

In this context, the defense of digital rights—such as privacy, freedom of expression, or identity—is not an end in itself. It becomes a **fundamental and contemporary strategy for the defense of territory, culture, and life** . Protecting a leader's WhatsApp account is not just an act of "personal cybersecurity"; it is an act of protecting the entire

community and its organizational process. Combating fake news about a prior consultation process is not just "fact-checking"; it is defending the legitimacy of their struggle and their right to self-determination. This module must, therefore, explicitly connect each digital right to the territorial defense agenda and the communities' life plans, imbuing this learning with a sense of urgency, relevance, and transformative power.

2.3 MODULE 3: TAKING CARE OF OUR DIGITAL MALOCA - COMMUNITY CYBERSECURITY

The goal is to develop practical skills and foster a culture of collective digital care, focusing on prevention, contextual risk identification, and the use of accessible, secure, and open-source tools.

2.3.1 Community Risk Map : What are we protecting ourselves from ?

The starting point for security is understanding the specific threats faced by the community. A dialogue will be initiated that connects risks already known in the physical world (threats, gossip, theft, surveillance) with their manifestations in the digital environment. The most common security incidents reported by human rights defenders in Colombia will be presented, including unauthorized access to devices and accounts, *phishing* (scams to steal credentials), and identity theft. [15] In addition, the alarming figure that 50% of the human rights defenders surveyed have received direct threats through digital means will be highlighted. [15] Particular attention will be paid to the differentiated risks that affect specific groups:

- **Young people:** Threats such as cyberbullying, dangerous viral challenges, and sextortion, which exploit the vulnerabilities inherent in adolescence, will be analyzed .
- **Women:** Online gender-based violence will be addressed, manifested through systematic harassment, non-consensual sharing of intimate images, and smear campaigns that attack women's credibility and participation in public life .

Practical Activity: Digital Risk Mapping

Inspired by participatory methodologies such as social cartography and body mapping, and adapting techniques from organizations like Tactical Tech [33] , this activity invites participants to visualize their risks. Using their preferred medium, they will be asked

to represent the community. They will identify and draw the digital threats that most affect them at the individual level (a Facebook account being stolen), family level (a young person being bullied in a WhatsApp group), and community level (a disinformation campaign against the local authority). This exercise provides a visual understanding of how a seemingly individual digital risk can have profound repercussions on the trust and cohesion of the entire community.

2.3.2 Basic Digital Hygiene and Care: Our First Steps

Fundamental safety practices will be taught in a simple, memorable, and immediately applicable way.

- **Strong and Unique Passwords:** Instead of complex and difficult-to-remember combinations, the technique of creating long, easy-to-memorize "passphrases" will be taught (e.g., "Myhousehas2dogsand1cat!"). The golden rule will be emphasized: a unique password for each important service .
- **Two-Factor Authentication (2FA): This crucial concept will be explained using the analogy of "putting two locks** on your front door." It will show how to activate 2FA for key services like WhatsApp, Facebook, and email, preventing unauthorized access even if someone steals your password.
- **Secure Browsing and Connection:** Students will be taught how to identify secure websites that use the https protocol (recognizable by the padlock icon in the browser). Students will be emphasized on the importance of being wary of suspicious links received via text or email and avoiding the use of public and open Wi-Fi networks for sensitive activities such as banking transactions or private communications .
- **Phishing Identification:** Through real-life examples adapted to the local context (e.g., a fake message about a government grant), participants will learn to recognize the signs of a phishing attempt: urgency, spelling errors, requests for personal information, etc.

2.3.3 Digital Guardian Toolbox: Free and Secure Software

A curated catalog of digital tools will be presented that are open source (allowing for auditing and building trust), free, and, crucially, designed to work efficiently in low-connectivity conditions. The selection is based on recommendations from trusted, expert organizations in the fields of human rights and technology, such as Security in a Box, the Electronic Frontier Foundation (EFF), SocialTIC, and Amnesty International .

Practical Activity: Installation and Configuration

This is an eminently practical session. With the guidance of facilitators, participants will install and configure these tools on their own devices (if they have them) or on community computers. The goal is to ensure they not only become familiar with the tool, but also learn how to use and configure it securely from the very beginning.

2.3.4 Digital Care Tools Catalog

The following table serves as a quick, visual, and easy-to-understand reference sheet, justifying the choice of each tool and empowering users to make informed decisions.

Name and Function	Why Did We Choose Her?	Where do I get it?	A Key Tip
Signal: For private and secure chatting and calling.	Free, end-to-end encryption by default, doesn't save your messages, works well with low data, recommended by human rights advocates. [35]	Play Store, App Store, Official Site	Activate "Registration Lock" (Security PIN) so no one else can register your number on another phone.
KeePassXC: To save all your passwords in one secure place and without the need for internet.	Free, open source, and works offline, giving you greater control and security over your data. Ideal for areas with poor connectivity ·	Official Site (for PC)	Save your database file in a safe place and create a backup copy on a USB flash drive. Don't forget your master password!
ProtonVPN: To protect your internet connection, especially when using public Wi-Fi.	· logs policy. Based in Switzerland, with strong privacy laws.	Play Store, App Store, Official Site	Always use it when connecting to a Wi-Fi network other than your home or a trusted network (e.g., in a park, internet cafe, airport).
Cryptomator: Create a digital "safe" and protect your important files on your computer, USB drive, or in the cloud.	Free, open source, easy to use. It encrypts files before uploading them to services like Google Drive or Dropbox, giving you an extra layer of security ·	Play Store, App Store, Official Site	Create a vault for your organization's or community's most sensitive documents. That way, even if someone accesses your cloud account, they won't be able to read the files.

Cybersecurity, in its traditional approach, focuses on the individual: "protect *your*

password," "install an antivirus on *your* computer." However, this perspective is insufficient and often inadequate for community contexts such as those of Indigenous and Afro-descendant communities, where well-being is a collective issue and the security of an individual is intrinsically linked to the security of the group. A report by the Karisma Foundation emphasizes that the lack of collective security protocols is a more serious problem than the lack of appropriation of tools by individuals. [15]

A digital attack against a leader is not an isolated attack; it is an attack against the organization, the process, and the community as a whole. [44] Therefore, the response must necessarily be collective. This module must transcend the paradigm of "individual self-protection" to build a framework of **"collective digital care** ." This approach reinterprets security practices as acts of solidarity and mutual responsibility. "I protect my WhatsApp account not only for my safety, but to protect the information of all my contacts and not put my community at risk." Practices such as security reviews in pairs, the creation of "circles of trust" to share alerts and support each other, [44] and the definition of shared responsibilities, such as designating one person to help others update their applications, should be promoted. In this vision, the "digital maloca" (the online community space) is cared for in a minga, with the effort and commitment of everyone.

2.4 MODULE 4: LA MINGA/CABILDO DIGITAL - INTERNET GOVERNANCE AND COMMUNITY PARTICIPATION

Objective: Empower participants to recognize themselves as legitimate and necessary actors in Internet governance, providing them with the knowledge and tools to influence policies and decisions that affect their digital lives and their territories, reinforcing community digital autonomy with the ability to decide on the use of platforms, data and technologies based on their own governance principles

2.4.1 What is Internet Governance and Why Do We Care?

Recapitulating the concepts from Module 1, we will delve deeper into the idea that "internet governance" is the process by which various actors (government, businesses, civil society, etc.) make decisions about the rules of the game in the digital world. [19] To ensure

that this concept is not abstract, we will use concrete examples that directly impact the lives of communities:

- The decision on the price of mobile data plans.
- Regulations that require (or not require) platforms to remove hateful and racist content.
- The allocation of public funds to connect rural schools.
- Copyright laws that may affect how ancestral knowledge is shared.

The central message is clear: if communities do not participate in these discussions, others will make decisions for them, and those decisions are likely not to reflect their needs, values, or rights. [47]

2.4.2 The Colombian Internet Governance Roundtable: A Space for Influence

The Colombian Internet Governance Roundtable will be presented in detail as the main national forum for this dialogue. Its purpose will be to explain who participates (representatives from the Ministry of ICT, the CRC, companies such as Google, and civil society organizations) , [19] and how it works. Its voluntary, non-hierarchical nature and its objective of promoting dialogue rather than imposing consensus will be highlighted. [47] The topics typically discussed will be reviewed, such as freedom of expression, cybersecurity, access, and copyright. [19] Critically, one of its greatest challenges will also be acknowledged: the need to include more and better voices from regions and ethnic communities, which have historically been underrepresented. [47]

Practical Activity: Analyzing the Minutes of the Board Meeting

To demystify this space, often perceived as technical and distant, we will work with a simplified excerpt from the actual minutes of a meeting of the Roundtable (publicly available on its website [47]). In groups, participants will read the excerpt and identify who spoke, what positions they defended, and what interests might be behind each intervention. This activity provides a practical understanding of the dynamics of the debate and the importance of preparing solid arguments for participation.

2.4.3 Building Our Agenda: From Complaint to Proposal

This submodule focuses on developing core skills for community advocacy, adapted to the digital ecosystem. The process is structured in clear and simple steps:

1. **Identify and Diagnose the Problem:** Based on the mapping and discussions from the previous modules, a problem is clearly defined. For example: "In our area, the internet signal is intermittent and the rates are the highest in the region, which prevents our youth from accessing online education."
2. **Gather Evidence:** Learn how to support the problem with data. This can include the connectivity maps developed in Module 1, community testimonials, tariff comparisons, etc.
3. **Formulate a Clear and Concrete Proposal:** The complaint becomes a request. For example: "We request that the Ministry of ICT and the CRC include our community in the next phase of the Internet Boards program and that a social rate be established for data plans in ethnic territories." [11]
4. **Interoperability between knowledge:** This axis reflects on how to generate a real dialogue between international frameworks, such as global internet governance, and community-based forms of organization specific to communities (assemblies, minkas , town councils, etc.). Communities do not always integrate into these processes in the same way: for example, installing infrastructure without active participation can generate detachment. On the other hand, when it is built collectively, as in a minga (a community meeting), where the community adapts the space and makes decisions, the technology becomes part of the territory and generates ownership.

   Before coordinating with allies, it is also important to recognize that each community has its own dynamics: in some cases, a call from the town council does not convene, but the local priest does. Beyond the minka (a community meeting), there are other forms of organization and participation, such as speaking circles, knowledge exchanges, house-to-house visits, or festive gatherings. These strategies allow for strengthening dialogue based on trust, culture, and mutual respect. Understanding them is key to fairer and more effective interoperability between knowledge.
5. **Identify and Coordinate with Allies:** No fight is fought alone. Identify potential allies: other communities with the same problem, civil society organizations working on digital rights · academics, journalists, or even local officials.
6. **Selecting an Advocacy Channel:** Different strategies for presenting the proposal are explored: formally presenting it to the Governance Board, conducting a social media campaign to raise awareness of the problem, contacting a congressperson in the region, etc.

Practical Activity: Developing a Proposal for the Digital Minga

Working on a real and priority issue for their community, participants will work in

groups to develop a one-paragraph advocacy proposal, following the five-step structure. They will then present it to the rest of the group, who will act as a panel of decision-makers, offering constructive feedback.

It is important to explicitly mention the right to technological and data sovereignty of Indigenous and Afro-descendant peoples as part of their participation in digital governance. This provides a more solid political framework.

To conclude, it is important to generate practical evidence: for example, each participating community should develop a proposal for its own digital governance principles or a symbolic digital town hall meeting.

2.4.4 Beyond Colombia: Regional and Global Spaces

To broaden the perspective and connect local struggles with a broader movement, the existence of governance forums at the regional level, such as the Latin American and Caribbean Internet Governance Forum (LACIGF), and at the global level, such as the United Nations Internet Governance Forum (IGF), will be briefly mentioned. [46] This helps participants understand that their challenges are not unique and that there is a global network of people and organizations working on similar issues, opening doors for international learning and solidarity.

Indigenous and Afro-descendant communities in Colombia have legally recognized self-governing structures, such as Cabildos and Community Councils, which are governed by life and ethnodevelopment plans that guide their future. The language and logic of formal internet governance spaces, with their *multi-stakeholder model* and search for consensus , may seem alien to these forms of organization. Simply inviting communities to "participate" in the Bogotá Roundtable could be interpreted as an attempt to assimilate [them] to an external model, rather than a strengthening of their own.

Initiatives such as the Juntanza Étnica program demonstrate that the most effective path is to strengthen “self-government and institutionality” and “self-determined economic development.” [49] Therefore, this module must reorient its focus. The central question should not only be “how do we bring our voice to the Mesa in Bogotá?” but, primarily, **“how do we make decisions about technology here, in our territory, according to our own norms and life plans?”** Participation in external spaces such as the Mesa then becomes a decisive and articulated strategy from self-government, not the ultimate objective.

The “Minga/Cabildo Digital” is not just a metaphor; it is the proposal to convene community assemblies to debate and decide on their digital future, thus exercising their right to self-government also in this new territory.

2.5 MODULE 5: WEAVING CARE NETWORKS - INCIDENT RESPONSE PROTOCOLS

The goal is to co-create a digital security incident response protocol that is simple, actionable, and tailored to the community's reality, strengthening collective resilience against attacks and transforming moments of crisis into opportunities for organizational strengthening.

2.5.1 What is an Incident and When is the Alarm Activated?

For a protocol to be effective, it must first clearly define what constitutes a "digital security incident" in the community context. It's not just a complex technical hack. An incident is any event in the digital environment that puts an individual, an organizational process, or the community as a whole at risk. Specific examples include:

- A direct threat received via WhatsApp or Facebook.
- The spread of a false rumor or a smear campaign against an authority or a community project.
- The theft or loss of a cell phone containing sensitive information (contacts, photos, documents).
- The creation of a fake social media profile that impersonates an organization or leader to create confusion.

Once the incident has been identified, it is crucial to assess its severity. Risk levels (low, medium, high) will be established based on two main criteria: the credibility of the threat and the potential impact it could have on the individual or the community. [44]

Practical Activity: Classifying Cases

Participants will be presented with several digital incident scenarios. In groups, they will discuss and classify each case according to the risk level, justifying their decision. For example: Is an anonymous insult in a Facebook comment more serious than a private

message with a death threat from an identified profile? This discussion helps develop a collective approach for decision-making under pressure.

2.5.2 The Rapid Response Protocol: A 5-Step Plan

A clear and memorable protocol structure will be presented, adapted from professional incident response frameworks [53] and practical guides designed for activists and human rights defenders. [44]

1. **Step 1: Contain and Assess (Don't Panic!):** The first reaction to a crisis should not be impulsive. The most important thing is to protect the affected person and prevent the damage from spreading. This may involve immediate actions such as disconnecting a device from the internet, notifying the threatened person to take physical precautions, or temporarily changing a password. A quick assessment should be made: What happened? Who is affected? Is the risk still present? [44]
2. **Step 2: Document the Evidence:** This step is crucial. Save as much evidence of the incident as possible: take screenshots of messages or profiles, save links (URLs), and note down dates, times, and usernames. Good documentation is essential for any subsequent formal reporting to the platforms or authorities ·
3. **Step 3: Communicate to the Circle of Trust: No one should face a crisis alone. It's vital to activate a previously defined internal support** network . The concept of a "circle of trust" or "care network" will be established, a small group of people within the community who must be notified immediately. This circle is the first ring of response and support.
4. **Step 4: Analyze and Eradicate:** Once the initial emergency has been contained and with the support of the trusted circle, the situation is analyzed more calmly to decide on the next steps. This may include blocking the offending user, reporting the post or profile to the platform, changing all related passwords, or performing a more in-depth analysis of the device if malware is suspected ·
5. **Step 5: Recover and Learn:** The response doesn't end when the threat is eliminated. It's critical to provide support to the affected person, recognizing that digital attacks have a real emotional and psychological impact. [44] Finally, the circle of trust and the community must reflect on what happened: What went wrong with our security practices? What can we do differently to prevent this from happening again? This collective learning step is what allows the protocol and the community to grow stronger with each experience. [53]

2.5.3 Creating Our Own Community Protocol

There is no one-size-fits-all protocol. Each community must design and adapt its own response plan based on its capabilities, resources, organizational structure, and the specific risks it faces. The *Earth Defenders Toolkit 's guiding questions will be used* to facilitate this co-creation process: Who are our closest allies? Who can we call in an emergency? Who are our opponents and what kind of tactics do they use? What is our most sensitive information that we must protect? [55]

Practical Activity: Designing the Community Protocol

Using a simple visual template (a "canvas"), participants will complete the fields of their own community protocol. This practical exercise will allow them to materialize the plan, defining key elements such as: the names and contacts of the people who make up the circle of trust, the name and number of the partner organization they can call for technical or legal advice (e.g., FLIP, SocialTIC), and the contact information of the relevant local authority (e.g., the captain of the Indigenous guard, a member of the community council).

2.5.4 Alert Follow-up: Community Rapid Response Protocol Template

This template is not a bureaucratic document, but rather a visual and tangible working tool. It can be printed and posted in a visible location at the community headquarters, serving as a quick action guide in times of crisis.

Rapid Response Protocol - Digital Guardians

1. INCIDENT (What happened?):
(Space to briefly describe the event)

---

2. RISK LEVEL: (Mark with an X)
( ) LOW ( ) MEDIUM ( ) HIGH

3. STEP 1: CONTAIN (Immediate Action)

- [ ] Notify the affected person.
- [ ] Disconnect the equipment from the Internet.
- [ ] Change master password.
- Other: _

4. STEP 2: DOCUMENT (Save Evidence)

- [ ] Take screenshot.

- [ ] Save link (URL).
- [ ] Write down the date, time and user.
- Other: _

5. STEP 3: COMMUNICATE (Who do we call?)

- **Internal Circle of Trust:**
  - Name: _ _ _ _ _ _ _ _ Contact: _ _ _ _ _ _ _ _
  - Name: _ _ _ _ _ _ _ _ Contact: _ _ _ _ _ _ _ _
- **External Support (Allies):**
  - Organization: _ _ _ _ _ _ _ _ Contact: _ _ _ _ _ _ _ _
- **Self-Authority:**
  - Position: _ _ _ _ _ _ _ _ Contact: _ _ _ _ _ _ _ _

6. STEP 4: ACTION (What do we do now?)

- [ ] Block user/profile.
- [ ] Report to the platform.
- [ ] Delete post.
- [ ] Review privacy settings.
- Other: _

7. STEP 5: LEARN (Lesson for next time)

(Space for collective reflection on how to improve)

Incident response protocols in the corporate or government world are typically technical and managerial procedures focused on efficiency and mitigating damage to the organization. [53] However, for a community, a digital incident, especially a threat or disinformation attack, is a deeply traumatic event. It generates fear, sows distrust, and has the potential to fracture the social fabric and paralyze organizational processes.

The response, therefore, cannot be merely technical; it must also be emotional, social, and political. The need for psychosocial support is an explicit and vital component of safety protocols designed for journalists and activists, who face similar pressures. [44] In this sense, the creation and practice of a protocol in a community context must be framed not as a bureaucratic exercise, but as a **ritual of collective care and empowerment** . Regularly practicing the protocol through drills not only improves the technical response, but, crucially, builds trust, reduces fear by making the existing support network visible, and reaffirms the bonds of solidarity. When a real incident occurs, the community reacts not from individual panic, but from a shared and rehearsed practice. In this way, the protocol becomes a tangible manifestation of the group's organizational cohesion and resilience, transforming a vulnerability into an opportunity for empowerment.

2.6 MODULE 6: THE ROLE OF THE COMMUNITY TRAINER OF FACILITATING KNOWLEDGE

Objective: To equip new trainers with the pedagogical, methodological, and planning tools necessary to successfully replicate this curriculum in their own communities, creatively and appropriately adapting it to their specific contexts.

2.6.1 The Art of Facilitating: Principles of Adult Education

For replication to be effective, new trainers must master the principles of andragogy (adult education), which recognize that adults learn differently than children. [2] Key principles to internalize are:

- **Building on Experience:** The most meaningful learning for adults occurs when new knowledge connects directly to their life, professional, and community experiences. The trainer should act as a bridge between the participants' experience and the new concepts
- **Active and Participatory Learning:** The "presentation" or "magisterial lecture" model, where the trainer speaks and everyone else listens, must be overcome. It is crucial to use active methods that promote discussion, collaborative exploration, problem-solving, and learning through doing. [2]
- **Creating an Environment of Trust and Respect:** The role of the trainer is not that of an expert who possesses all the truth, but rather that of a facilitator who guides a process of collective discovery. This requires attitudes of active listening, respect for all opinions, empathy, and humility to learn from the participants as well. [4]

2.6.2 Planning the Replication: From Idea to Training Action

Participants will be guided through a complete planning cycle, providing them with a roadmap for organizing their own workshops

1. **Needs Analysis:** The first step is to ask yourself: What is most urgent and relevant for my community right now? Do they need to focus more on the security tools in Module 3 due to recent threats? Or is understanding internet governance from Module 4 more of a priority to influence a local project [?]
2. **Defining Learning Objectives:** Based on needs, define clear and achievable objectives. What do I want participants to know, feel, or be able to do by the

end of the workshop ?

3. **Activity Design and Adaptation: We'll teach you how to not only replicate the activities in this curriculum, but also how to adapt** them . Do the analogies used here work in my community, or should I create others? What local cases or examples can I use to make the concepts more relatable? Contextualization is key, especially in rural and indigenous settings.
4. **Materials Preparation and Logistics:** You should plan the necessary resources in advance. Do I need to print the tables and templates? Do I have access to a projector? How can I facilitate the workshop if there's no electricity or internet connection ?
5. **Participatory Assessment: Assessment is not an exam. Simple, participatory methods will be taught to evaluate whether the objectives were met, such as rounds of final word, drawings depicting what has been learned, or short role** - plays where knowledge is applied.

2.6.3 The Trainer's Toolbox

A set of practical resources and techniques for facilitation will be provided:

- **De-escalation Techniques:** Icebreakers to get things started, energizers for moments of fatigue, and techniques to encourage orderly and productive discussion in small groups ·
- **Group Management:** Strategies for managing different personalities in a group: how to moderate a talkative participant, how to encourage shy participants to participate, and how to mediate potential conflicts or disagreements ·
- **Content Adaptation:** Skills to simplify technical language, create new metaphors and analogies that resonate with local culture, and contextualize examples. Emphasis will be placed on the importance of adapting materials to the specificities of rural areas ·
- **Using Offline Resources: Creative strategies for teaching about technology without relying on it will be explored, using tools such as flip charts, concept cards, theater of the oppressed** · and other dynamics that do not require an internet connection or digital devices.

Final Practical Activity: “My First Workshop”

As a culmination of the training process, each participant (or small groups) will have the opportunity to design and facilitate a 15- to 20-minute micro-session on one of the curriculum topics. This practical exercise will allow them to apply everything they've learned and receive constructive feedback from their peers and the lead facilitator. This activity serves

as a rite of passage, consolidating their confidence and their identity as new community "Trainers of Trainers."

The traditional Training of Trainers model often focuses on the faithful replication of predefined content. [3] However, this approach is inadequate for the vast cultural, social, and contextual diversity of Indigenous and Afro-descendant communities in Colombia. A "one-size-fits-all" curriculum is destined to fail. Research on technology-mediated education in rural and Indigenous contexts demonstrates that the key to success lies in the ability to contextualize and adapt pedagogical proposals to each reality. [60] The role of the Indigenous Teaching Assistant (ADI) in some educational models is precisely that of an interpreter and cultural bridge. [60]

The real challenge for the new Digital Guardian will not be to memorize the content of this curriculum, but to reinvent it and creatively adapt it to their community. Therefore, this final module must redefine their role. They are not simply a "content replicator" but a **"cultural translator"** and a **"network weaver** . "

- As a **cultural translator** , your most valuable skill will be taking the universal concepts of cybersecurity, rights, and governance and translating them into the language, metaphors, values, and logic of your own people. Your success will depend on your pedagogical creativity in making knowledge relevant and meaningful.
- As a **networker** , your work doesn't end at the end of a workshop. Your role is to keep the conversation going, connect participants in your community with the broader network of Digital Guardians being formed in other regions, and serve as a bridge with partner organizations. Your role is to continue strengthening the digital care network at the local, regional, and national levels.

Ultimately, this curriculum not only seeks to deliver knowledge, but also to initiate and nurture a movement of communities that critically embrace technology to defend their rights and strengthen their autonomy.

3- CONTINUOUS UPDATING OF THE CURRICULUM FOR EFFECTIVE RESULTS

It is understood that the curriculum provides the necessary foundation for teaching digital security, internet governance, and digital rights, encompassing the realities of

Indigenous Peoples, Afro-descendants, and rural and urban communities. However, it is important to emphasize that those implementing the curriculum must update it to reflect the local or regional realities where the content is applied, as there may be minor differences that require attention.

As effective outcomes of a curriculum capable of training individuals to become trainers, we hope to generate greater community empowerment in digital matters, reducing the risks of insecurity and teaching them how to implement new tools to be developed in courses, training sessions, or other training spaces.

4- EVALUATION AND IMPACT MEASUREMENT METHODS

To ensure the curriculum's effectiveness and measurability, it is proposed that content applicability and the use of proposed knowledge be measured from beginning to end. Regarding impact, by assessing the level of confidence and knowledge, it is possible to measure which curriculum and course materials will have the greatest impact.

4.1 EVALUATION METHODS

To evaluate the curriculum, online meetings are proposed with experts (on digital security, internet governance, and the realities of local communities) and interested individuals/students. This method allows for the identification of specific needs and expectations. It will be implemented through initial surveys, brief interviews, or practical diagnostic exercises, which makes it easier to adapt the content to the reality of the target group for the training of trainers who will subsequently use this curriculum.

In addition, formative assessment is also proposed as a method. Throughout the training and use of the curriculum, it will be carried out continuously in each module through activities and exercises on forms that measure both knowledge and content relevance. Its purpose is to provide feedback to both the trainer and participants, adjusting the pace and methodologies to maximize learning.

4.1.1 Meeting Guide

The purpose of the meetings is to create a safe, participatory space where experts, or experts and students, can exchange perceptions about the curriculum, identify successes, identify gaps, and propose improvements. It is recommended that these meetings be held at different stages of the process (at the beginning, middle, and end) to measure learning progress and the cultural relevance of the content. To guide the discussion, guiding questions such as:

- What parts of the curriculum could be improved? What content is missing?
- Are there topics that should be explained in more depth or examples that are closer to local reality?
- Are the technical and ethnic concepts adequate? Is there anything that needs to be adapted or changed to make it more effective and applicable?
- How easy and clear is it to apply the acquired knowledge in everyday community life?
- What improvements could be implemented to strengthen the curriculum?

It is important that meetings be moderated using participatory methodologies (talking circles, brainstorming, collective prioritization) so that all voices are heard and the responses collected can be systematically documented to inform program evaluation and feedback reports.

4.1.2 Key questions for forms

Evaluation forms allow for the collection of systematic and comparable information on the training process. It is recommended that they be brief, accessible, and administered at various times (initial assessment, during each module, and at the end of the process). The questions should focus on both the level of knowledge and the relevance and applicability of the content. Some examples of key questions are:

- What level of prior knowledge do you have about digital security and internet governance?
- What are your main expectations regarding this training?
- How useful do you consider the content of the module worked on for your community?
- Which topics did you find most difficult or least clear?

- Do you have any suggestions, comments, or questions about the modules?
- How do you intend to implement the learnings from this course as a community trainer/facilitator?
- Do you think you can apply the knowledge acquired in the course in practice in your daily community life?
- Do you have any suggestions for a topic that should be included in the course?
- How do you rate your satisfaction with the course?
- Do you have any suggestions, comments or questions about the course/curriculum?

The important thing is that the results are analyzed jointly by the coordination team to provide feedback on the methodology and measure the curriculum's real impact on community capacity building.

4.1.3 Virtual workshop on digital security risk mapping

As a tool for future curriculum implementers (especially CSOs working with indigenous and Afro-descendant peoples in Colombia) who wish to validate the curriculum and its information, a third possible method is also suggested, which is carried out through a workshop in the format shown below.

VIRTUAL DIGITAL SECURITY RISK MAPPING WORKSHOP (90 MINUTES)

The goal of the workshop is to uncover and prioritize risks (not solutions): *asset/value* + *threat/actor* + *condition/vulnerability* + *consequence* . This structure is aligned with risk assessment frameworks widely used in CSOs.

0) PREPARATION (BEFORE THE SESSION)

- **Call and consent** (no recording, pseudonyms allowed).
- **Low connectivity plan:** audio first; whiteboard → Google Sheets/Forms; backup channel via WhatsApp.
- **Roles:** facilitation, co-facilitation/rapporteurship, technical support, interpreter(s) if applicable (indigenous language).

- **Intercultural approach:** If **sensitive knowledge/archives are touched upon** , only name categories (“ritual chant,” “sacred map”) without details unless community authorization is obtained.

1) THE SESSION (WITH CONNECTIVITY)

A. Safe opening and rules (5')

- Agree: no recording; use pseudonyms if preferred; intercultural respect.
- Connectivity quality query via chat: 🟢 / 🟠 / 🔴 .
- **Low connectivity mode:** audio responses; speaker takes notes on Sheet.

B. Discovery of assets and flows (15')

Broad trigger: “Imagine if internal information about your organization (contact lists, meeting photos, advocacy plans, meeting minutes) appears on the internet tomorrow. What would be *more serious* than it being made public or lost?”

Concise questions:

- What things would be critical if they were lost or published?
- Where does that information “live” today (own phone/OSC, USB, cloud, computer)?
- Who uses them and with whom are they shared (roles, not names)?
  Capture (narrator): Asset table – *Location – Who uses – Who is shared with* + **preliminary impact** (High/Medium/Low).

C. Context and actors (10')

Trigger: “During the referendum/election season, new accounts appear that attack the community; there are also extractive interests nearby.”

Questions: What tense situations are there? Who might want to stop your work or look at your data (ally/neutral/potential aggressor)?

Capture: *Actor – Motivation – Ability (B/M/A) – Asset that interests you* .

Objective: Map plausible threats for probability calculation .

D. Incidents and signals (15')

Cases in simple language (choose 3):

- *Scam by message/email* : "It seems to be from an entity, it asks to "verify password" with a link."
- *File that makes the computer sick* : "I opened 'list.xls' and the computer became slow/strange windows appeared."
- *Impersonation* : "profile with photo of the leader asked for money/data."
- *Doxxing/mocking* : "they published someone's phone number/address."
- *Cell phone signal cut off or checked* on the day of an assembly.

Questions: Did something similar happen? **Yes/No/I don't know** . When? (≤3m / 3–12 / >12). What did it affect (people, reputation, files, activity)?

Capture: *Event – Date – Channel – Active – Consequence* .

Rationale: prioritize by recency and frequency.

E. Key accounts and dependencies (10')

Simple explanation (1'): *Key accounts* = master keys that open critical systems. Examples:

- **Institutional email** (admin who creates or deletes accounts).
- **Social networks** (page/profile owner).
- Website **domain and hosting (who pays/renews).**
- **File cloud** (who can invite/kick).
- **Banking/donations** (access to transactions).

Questions: Which ones exist? Who has the key? Is there a backup or recovery option? Do any of them depend on a single team or person?

Capture: Critical Resource list – *Who has the key (role) – Backup/Recovery? – Unique dependency (Yes/No)* .

Objective: Reduce single points of failure in the analysis.

F. Public exposure and controversial issues (10')

Trigger: "A post about land/environment generated hundreds of hostile comments and aggressive private messages."

Questions: What public channels do they use (web, Facebook, TikTok, radio)? What topics trigger attacks? Recent fake profiles?

Capture: List of **hot channels** with date/topic.

Objective: Inputs for reputational/legal and impersonation risks.

G. Prioritization (20')

Methodology: probability×impact scheme used in organizational assessments.

- The reporter converts responses into **risk statements** :
  "There is a risk of **[threat/actor]** against **[asset]** due to **[condition]** , with **[consequence]** ."
- Quick vote (chat): Each person marks 3 risks they consider **most likely** and 3 with **the greatest impact on people/culture/operations** .
- The facilitation team cross-references votes and incident **recency to compile a Top-10** .

H. Closing (5')

- Top-10 Review (read only).
- Explain what will happen to the data (custody/anonymization).
- Reminder of **help channels** (helplines and resources).

3) LOW CONNECTIVITY MODE

Considering the scenario where there are many people, communities, and organizations with low connectivity, we propose different ways to run the session:

- **Video optional;** audio only if there are interruptions.
- **Whiteboard → Google Sheets** (tabs: *Assets, Actors, Incidents, Key Accounts, Risks*).
- **WhatsApp responses** with short codes

4) PRODUCTS AND RESULTS

As products leaving this session (in both modes - with connectivity or low connectivity):

- Identification of specific needs (through: Risk matrix, Incident log from the last 12–18 months, Top-10 prioritized risks);
- Curriculum feedback (through: Stakeholder map - motivation/capacity, list of key accounts and unique dependencies).

4.2 IMPACT ASSESSMENT

This evaluation seeks to measure whether the curriculum generates sustainable changes in community practice. It will be implemented by monitoring indicators such as:

- Number of documents, templates or models created;
- Number of meetings and training for communities;
- Adoption of collective digital security protocols.
- Community advocacy cases in internet governance.
- Perception of greater security and digital autonomy on the part of participants.

With this approach, the evaluation is not limited to measuring individual results, but becomes a participatory, transparent process aimed at strengthening the digital autonomy of communities.

REFERENCES

1. The triple barrier to bridging the digital divide for Indigenous peoples - What if we talk about equality?, https://blogs.iadb.org/igualdad/es/brechas-digitales-pueblos-indigenas/
2. Training for Trainers (TfT) Training Methodology, https://ec.europa.eu/programmes/erasmus-plus/project-result-content/cb5685ff-4c8a-4ae0-8d3f-dfee5c3dc3fe/AgriSafetyNet_Training_Methodology_IO3_ES.pdf
3. TRAINING OF TRAINERS - ILO/Cinterfor, https://www.cinterfor.org/sites/default/files/file_publicacion/manual_seg.pdf
4. Training of trainers, http://www.halinco.de/html/proy-es/mat_did_1/form_form.htm
5. Training of Trainers - OCW, https://ocw.ehu.eus/pluginfile.php/47292/mod_resource/content/1/Guia_Docente.pdf
6. Redalyc. Popular Education: A collective construction from the South and from below, https://www.redalyc.org/pdf/2750/275031898079.pdf
7. Popular Education: An Overview - Info CDMX, https://infocdmx.org.mx/escuela/curso_capacitadores/educacion_popular/decisio10_saber1.pdf
8. ACTION RESEARCH AND POPULAR EDUCATION - Hegoa Library, https://biblioteca.hegoa.ehu.eus/downloads/21409/%2Fsystem%2Fpdf%2F4576%2FM-7054.pdf
9. Popular Education in the Struggles for Human Rights in Latin America - DVV International, https://www.dvv-international.de/en/adult-education-and-development/editions/ead-72-2009/contributions/popular-education-in-the-struggles-for-human-rights-in-latin-america
10. Popular Education in the 21st Century: Intercultural Resistance from the South and Below - SciELO Colombia, http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S2216-01592015000200006
11. Through 19 Connectivity Communities – Internet Boards, the most remote homes in Vaupés will be connected - MinTIC, https://www.mintic.gov.co/portal/715/w3-article-397578.html
12. Report to Congress MinTIC 2023 – 2024 - Chamber of Representatives, https://www.camara.gov.co/sites/default/files/2024-11/INF-DE-GESTION-MIN-TIC.pdf
13. Latin America in a glimpse of the Amazon - Digital Rights, https://www.derechosdigitales.org/wp-content/uploads/DD_Amazonia_3_Colombia.pdf
14. Internet access in dribs and drabs: Indigenous peoples' digital divide in ..., https://www.dejusticia.org/acceso-a-internet-en-la-amazonia/
15. BETWEEN DISCONNECTIONS AND RISKS: BETWEEN ..., https://web.karisma.org.co/wp-content/uploads/2024/12/Informe-seguridad-digital-k-lab.pdf
16. Digital risks to which children are exposed and how to prevent them - ICBF,

https://www.icbf.gov.co/ser-papas/riesgos-digitales-los-que-se-exponen-los-ninos-y-como-prevenirlos

17. Colombian youth fight for digital education without social or racial barriers for indigenous students | UN News, https://news.un.org/en/story/2021/02/1487982
18. impactok23.pdf - Karisma Foundation, https://web.karisma.org.co/wp-content/uploads/2024/10/impactok23.pdf
19. Internet governance as a platform for advancing ICT-based education policies. The case of Colombia | Opera, https://revistas.uexternado.edu.co/index.php/opera/article/view/5127/6819
20. Governance - .CO Domain - MinTIC, https://gobernanzadeinternet.mintic.gov.co/752/w3-propertyvalue-198152.html
21. Digital Inclusion and Internet Content Governance - Organization of American States, https://www.oas.org/en/iachr/expression/reports/Digital_inclusion_eng.pdf
22. Report on Digital Inclusion and Internet Content Governance - Organization of American States, https://www.oas.org/es/cidh/expresion/informes/Inclusion_digital_esp.pdf
23. What digital rights exist and why are they important? - European University, https://colombia.universidadeuropea.com/blog/derechos-digitales/
24. Digital Health and Digital Rights in Colombia - COLEV - Universidad de los Andes, https://colev.uniandes.edu.co/images/documentos/IP-DRAG-ESP-Colombia-FINAL.pdf
25. Digital rights in Colombia: What are they and how are they regulated? https://colombia.unir.net/actualidad-unir/derechos-digitales/
26. Disinformation and online violence affect public conversation in Colombia - Publications and other publications | FLIP, https://flip.org.co/publicaciones/otras-publicaciones?item=desinformacion-y-violencia-en-linea-afectan-la-conversacion-publica-en-colombia
27. Index | The Digital Rights Index is an alliance of civil society organizations working on human rights issues in digital environments. The Index aims to catalyze the activities of its members and serve as a space for communication on urgent issues related to the exercise of these rights in Colombia. https://indicederechos.digital/
28. Content Moderation and Local Stakeholders in Colombia | Article 19, https://www.article19.org/wp-content/uploads/2024/05/v.2_ESPANOL_Content_Moderation_and_Local_Stakeholders_in_Colombia.pdf
29. Law passed in Colombia seeks to protect minors from the dangers of the internet: these are the new measures, https://www.infobae.com/colombia/2025/07/23/fue-sancionada-ley-de-entornos-digitales-sanos-que-busca-proteger-a-los-menores-de-edad-en-internet/
30. New Global Disorder: Digital Attacks on Freedom of Peaceful Assembly and Association, https://www.accessnow.org/press-release/nuevo-desorden-mundial-ataques-digitales-a-la-libertad-de-reunion-pacifica-y-asociacion/
31. Between disconnections and risks: digital security for people...,

https://web.karisma.org.co/entre-desconexiones-y-riesgos-seguridad-digital-para-las-personas-defenders-de-derechos-humanos-en-colombia/
32. Publications and other publications | FLIP, https://flip.org.co/publicaciones/informes
33. Property:Existing toolkits and resources, https://gendersec.tacticaltech.org/wiki/index.php?title=Property:Existing_toolkits_and_resources&until=Taller+de+cartograf%C3%ADa+y+security+digital+directed+to+women%2C+Oaxaca%2C+Mexico
34. View Information for Advocacy - SocialTIC, https://socialtic.org/wp-content/uploads/2017/06/VIFA_Espanol_Digital.pdf
35. Digital Security - Concepts and Basic Tools - May 2020.pdf - Related, https://conexo.org/wp-content/uploads/2020/06/Seguridad-Digital-Conceptos-y-Herramientas-Básicas-Mayo-2020.pdf
36. Digital Security Guide for Everyone - CAMECO, https://www.cameco.org/media/es_gu_a_de_seguridad_digital_para_todos-_cameco.pdf
37. SUPPORT GUIDE - UNODC, https://www.unodc.org/documents/Cybercrime/tools-and-resources/guia_de_apoyo_docentes_sp.pdf
38. 6 Types of Network Security Protocols - Check Point Software, https://www.checkpoint.com/cyber-hub/network-security/what-is-network-security/6-types-of-network-security-protocols/
39. Digital Security Tools | Puntal - UN-DH, https://hchr.org.mx/puntal/prevencion-y-proteccion/prevencion/seguridad-y-prevencion-de-riesgos/herramientas-de-seguridad-digital/
40. Digital Security Resources Platform - Amnesty International Security Lab, https://securitylab.amnesty.org/es/digital-resources/
41. Digital Security Resource Hub for Civil Society - Amnesty International Security Lab, https://securitylab.amnesty.org/digital-resources/
42. What do you need to protect? https://securityinabox.org/es/
43. Top 5 security apps to protect your data in 2025, https://preyproject.com/blog/5-apps-to-improve-data-and-device-security
44. Safety Protocols for Journalists - International Center for ..., https://www.icfj.org/sites/default/files/2022-12/PROTOCOLOS%20DE%20SEGURIDAD%20%28Final%2010-29-2022%29.pdf
45. Third Report on Internet Governance in Colombia - Communications Regulation Commission, https://crcom.gov.co/es/biblioteca-virtual/tercer-informe-gobernanza-internet-en-colombia
46. Support for Internet Governance Initiatives in Latin America and the Caribbean - LACNIC, https://www.lacnic.net/7101/1/lacnic/gobernanza-de-internet
47. Colombia | Global Information Society Watch, https://www.giswatch.org/en/country-report/internet-governance/colombian-bureau-internet-governance
48. Meeting of the Colombian Internet Governance Roundtable - ISOC, Colombia,

https://www.isoc.co/es/noticias/reunion-mesa-colombiana-de-gobernanza-de-internet

49. Strengthening Afro-Colombian and Indigenous Peoples in Colombia - Latin America Leadership Program, https://lalp.georgetown.edu/es/news/strengthening-afro-colombian-and-indigenous-peoples-in-colombia
50. Latin American and Caribbean Internet Governance Forum: What Challenges Does the Region Face? | Association for Progressive Communications, https://www.apc.org/news/latin-american-and-caribbean-internet-governance-forum-what-challenges-does-the-region-face ?
51. Latin American and Caribbean Internet Governance Forum (LACIGF) in Santiago, Chile, https://datosprotegidos.org/lacigf-stgo-chile/
52. Regional Forum on Internet Governance - LACIGF 2023 - Externado University, https://www.uexternado.edu.co/departamento-de-derecho-de-los-negocios/foro-regional-de-gobernanza-de-internet-lacigf-2023/
53. What is Incident Response? - IBM, https://www.ibm.com/mx-es/topics/incident-response
54. What is Incident Response? - IBM, https://www.ibm.com/en-us/topics/incident-response
55. Guide: Digital Security for Earth Defenders..., https://www.earthdefenderstoolkit.com/toolkit/digital-security-for-earth-defenders/?lang=en
56. Incident Response | INCIBE-CERT, https://www.incibe.es/incibe-cert/incidentes/respuesta-incidentes
57. Incident Response Guide - CISA, https://www.cisa.gov/sites/default/files/2024-05/WWS-Sector_Incident-Response-Guide_ES.pdf
58. What is the training of trainers and what are its main contributions to professional education? - ORT University Uruguay, https://ie.ort.edu.uy/blog/que-es-la-formacion-de-formadores-y-cuales-son-sus-principales-aportes-a-la-educacion-profesional
59. The training of trainers: The relevance of dialogic, recursive, and underlying processes - SciELO México, https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2448-84372017000100088
60. Technology-Mediated Rural Secondary Schools in ... - Unicef, https://www.unicef.org/argentina/media/10721/file/Secundarias%20Rurales%20Mediadas%20por%20Tecnolog%C3%ADas%20en%20la%20Argentina.pdf
61. The 4 C's: Principles for Technological Integration in Rural Schools, https://es.fabretto.org/las-cuatro-c-integracion-tecnologica/
62. Rural education mediated by traditional technology during the pandemic 2020-2022 | Between Science and Engineering - UCP Journal Portal, https://revistas.ucp.edu.co/index.php/entrecienciaeingenieria/article/view/2778
63. Rural education mediated by traditional technology in times of pandemic 2020-2022,

http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1909-83672022000100051