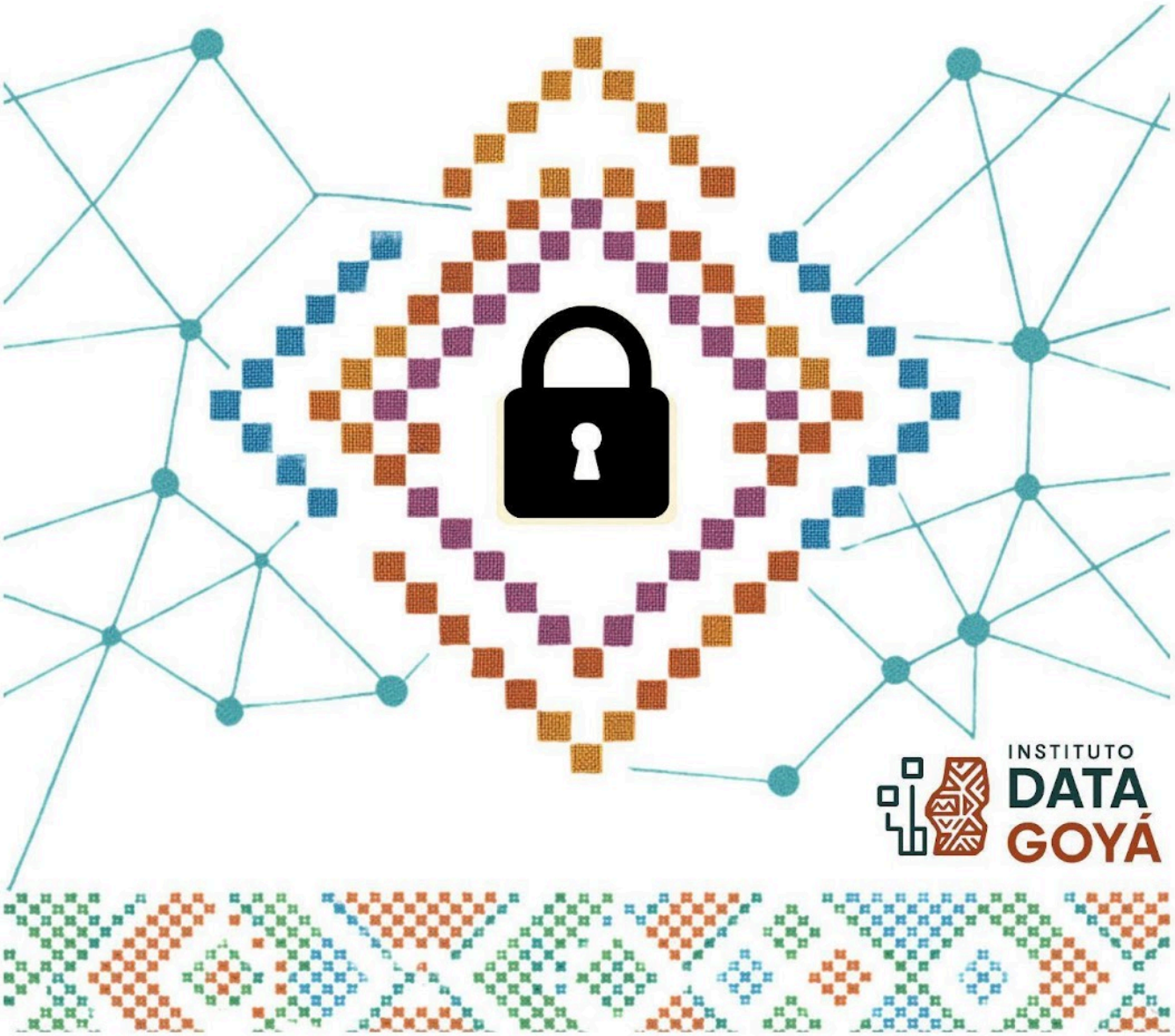
WEAVING DIGITAL SECURITY

TRAINING OF TRAINERS IN DIGITAL SECURITY FOR INDIGENOUS AND AFRO-DESCENDANT ORGANIZATIONS, COMMUNITIES, AND PEOPLES IN COLOMBIA: THE UNDERSTANDING, TRAINING, AND EMPOWERMENT IN CYBERSECURITY AND DIGITAL SOVEREIGNTY



September 2025

DATA GOYÁ INSTITUTE

Training of trainers in digital security for indigenous and Afro-descendant organizations, communities, and peoples in Colombia : understanding, training, and empowerment in cybersecurity and digital sovereignty / Denise Machado Leal ; content Denise Machado Leal, Umut Pajaro Velásquez, Jose A. Rojas Marcelo, Ximena Cuzcano, Saya Pastillo, Karen Gutiérrez, Isac Pulido ; style, design, and editing Denise Machado Leal. -- Rubiataba, Goiás, Brazil : Instituto Data Goyá, 2025. p. 26.

Includes references.
Version in English
Original Text in Spanish.

Work Identification Number: 082025 - Version of September 30, 2025

1. Digital Security - Training of Trainers - Colombia. 2. Cybersecurity - Study and Teaching - Colombia. 3. Digital Sovereignty - Colombia. 4. Indigenous Peoples - Digital Training - Colombia. 5. Afro-descendants - Digital Empowerment - Colombia.

CDD 370

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

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

Author
Denise Machado Leal

Content
Denise Machado Leal
Umut Pajaro Velásquez
Jose A. Rojas Marcelo
Ximena Cuzcano
Saya Pastillo
Karen Gutiérrez
Isac Pulido

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.

TRAINING OF TRAINERS IN DIGITAL SECURITY FOR INDIGENOUS AND AFRO-DESCENDANT ORGANIZATIONS, COMMUNITIES, AND PEOPLES IN COLOMBIA: UNDERSTANDING, TRAINING, AND EMPOWERMENT IN CYBERSECURITY AND DIGITAL SOVEREIGNTY

In collaboration with HIVOS, within the framework of the "Connect, Defend, Act" project in Colombia, the Data Goyá Institute and its team developed this Training of Trainers in digital security for indigenous and Afro-descendant organizations, communities and peoples in Colombia, which includes the following topics: Understanding, training and empowerment in cybersecurity and digital sovereignty, Introduction to digital security, studies on legislation and regulations on data protection applicable to CSOs, Identification of and response to the most common cyber threats faced by CSOs, Encryption tools and secure communication, and Risk mitigation strategies.

In addition, in designing the Training of Trainers program focused on digital security, we planned and delivered training sessions for selected students/trainers, covering key digital security concepts and adult learning methodologies. We also worked to provide trainers with teaching tools and resources, such as materials, presentations, and case studies.

The ToT plan includes methods for assessing trainers' preparation and ability to replicate the training with other groups. We are happy and proud of the final training product; we believe it can be easily used in other countries besides Colombia, so we want to recommend, promote, and participate in this process of expanding and replicating this valuable and unique material. Ultimately, the training becomes a sustainable and empowering digital security training. We thank HIVOS for the collaboration and opportunity, and we hope to bring this content to more countries.

SUMMARY

1. INTRODUCTION **6**
2. OBJECTIVES **6**
2.1 GENERAL OBJECTIVE 6
2.2 SPECIFIC OBJECTIVES 7
3. TARGET AUDIENCE **7**
4. METHODOLOGY **7**
5. TRAINING CONTENT **8**
6. ACTION PLAN 9
6.1 PLANNING 10
6.2 EXECUTION OF ONLINE TRAINING 10
6.2.1 The online course 11
6.2.2 Module 1: Our Digital Territory - Understanding the Internet Ecosystem 12
6.2.3 Module 2 – Our Rights in the Digital World 14
6.2.4 Module 3 – Caring for Our Digital Maloca: Community Cybersecurity 16
6.2.5 Module 4 – The Minga/Cabildo (Council) Digital: Internet Governance and Participation 19
6.2.6 Module 5 – Weaving Care Networks: Incident Response Protocols 20
6.2.7 Module 6 – The Role of the Community Trainer : Facilitating Knowledge 22
6.3. EXECUTION OF FACE-TO-FACE TRAINING 24
6.4 EXPECTED RESULTS 25
7. EVALUATION AND MONITORING 25
REFERENCES **26**

1. INTRODUCTION

Digital security has become an essential element for the protection of information, privacy, and the safe exercise of fundamental rights in the digital environment. Civil Society Organizations (CSOs), Civil Society Actors (CSAs), and leaders of peoples, communities, and collectives of Indigenous and Afro-descendant people, or those who work with them, in Colombia often find themselves in vulnerable situations, handle sensitive data, and face particular risks from digital threats.

In this context, this document is a detailed plan for training individuals capable of applying and replicating information on the topic of digital security. A training-of-trainers plan is designed as a sustainable strategy for building internal capacity in digital security. By empowering a group with strategies to act as trainers, the transfer of skills is ensured and the replication of these learnings in their communities and organizations is facilitated.

2. OBJECTIVES

The objective of the Training of Trainers (TBT) program is to build sustainable digital security training within CSOs by strengthening a group of community trainers, equipping them with the technical, pedagogical, and practical skills necessary to replicate the training independently and effectively. The training should present and teach technical topics in an accessible and useful manner, empowering trainers and students to take ownership of their digital rights, provide them with tools to control their data, and provide them with knowledge of digital and technological sovereignty.

2.1 GENERAL OBJECTIVE

The overall objective for training trainers is to strengthen community leaders' capacity in digital security strategically so they can replicate the knowledge they have acquired.

2.2 SPECIFIC OBJECTIVES

The program's objective is achieved through small, specific goals such as designing and implementing the strategic planning document, delivering training sessions, sharing a comprehensive set of teaching tools and resources (materials, presentations, case studies) with trainers, assessing trainers' capabilities, providing ongoing post-training support to ensure trainer confidence and capacity, and sending certificates and opportunity lists to participants.

3. TARGET AUDIENCE

The program is aimed at individuals associated with Civil Society Organizations (CSOs), Civil Society Actors (CSAs), and leaders of communities, communities, and collectives, within an ethnic perspective (indigenous and Afro-descendant people in Colombia). Priority will be given to participants committed to replicating the content within their organizations. We also seek to focus on individuals who represent cultural, linguistic, territorial, gender, and ethnic diversity to ensure that the training responds to different contexts.

No prior experience in community training or capacity building processes is required, as the course will include teaching methods and materials to support everyone in developing and implementing the training, even if they are beginners. We believe that, above all, even if a person doesn't replicate the classes in their communities but applies the strategies in their daily life and community, this application of digital security in daily life is a true educational replication of the content and empowers both the individual and those around them.

4. METHODOLOGY

The ToT methodology will be based on an approach that recognizes participants' prior experience and promotes active and collaborative learning. Popular education techniques

and participatory methodologies, such as simulations, case studies, and practical problem-solving, will be applied.

With a Hybrid approach, the FdG combines an online self-training phase (through the platform cursotejiendoseguridad-digital.com) with an intensive in-person component to consolidate practical skills.

The training will combine theoretical sessions with practical sessions, in which trainers will develop their own facilitation skills. The creation of a support network among trainers will also be encouraged to ensure mutual support and the exchange of experiences.

5. TRAINING CONTENT

The training program will include thematic and pedagogical modules that will allow trainers to acquire both technical knowledge and teaching skills. The suggested modules, based on the curriculum content [1], are:

2.1 Module 1: Our Digital Territory - Understanding the Internet Ecosystem
2.2 Module 2: Our Rights in the Digital World
2.3 Module 3: Caring for Our Digital Maloca - Community Cybersecurity
2.4 Module 4: The Minga/ Cabildo (Council) Digital - Internet Governance and Community Participation
2.5 Module 5: Weaving Care Networks - Incident Response Protocols
2.6 Module 6: The Role of the Community Trainer: Facilitating

The program, despite being very comprehensive, allows for changes and adjustments based on student feedback. Throughout the training, it is important to understand that knowledge is unfinished and is built collectively. The final version of the ToF is co-created and will be revised based on student feedback and perspectives. A traditional educational model, where knowledge is a one-stop shop and does not consider the reality and knowledge students bring, lacks innovation and is methodologically uninteresting.

[1] VELASQUEZ, Unnut Pajaro; MACHADO LEAL, Denise; ROJAS MARCELO, José A. Community digital guardians: a training of trainers curriculum in cybersecurity, governance, and digital rights for indigenous and Afro-descendant communities in Colombia. Content review: Unnut Pajaro Velásquez. Ethnic perspective review: Suya Corridor. Edited and styled by Denise Machado Leal. Rubiataba, GO: Data Goyá Institute, 2025

By valuing students' creativity, input, and knowledge, the ToT will be seen as more complete and democratic. It's not correct to speak of an ethnic perspective without including, listening to, and respecting those perspectives. In this sense, expert teachers and content providers must believe in and utilize an active teaching methodology.

6. ACTION PLAN

The action plan was designed to support participants in diverse territorial, cultural, connectivity, and digital literacy situations, so that participants not only acquire technical and methodological knowledge, but also develop confidence and practical capacity to replicate the learning in their organizations and communities.

The Digital Security Training of Trainers (ToT) strategy was conceived as a hybrid approach, combining an online training process with in-person training spaces. Given the lack of accessibility to fully in-person courses (given territorial issues) and poor connectivity in some regions of Colombia, offering hybrid training on a platform that doesn't require much internet access was the best option to ensure course accessibility.

Exploring websites and digital tools creates a connection with digital security, infrastructure, and technology content. Therefore, for the trainers who will read this document and also work to conduct their own Training of Trainers, we understand that even if logistical support for in-person activities is not available, it is interesting and important to use digital tools. Training is not just about teaching, but also about testing knowledge and digital literacy.

We understand that over time and with implementation in different spaces, the training of trainers plan will change and transform for the better, based on the reality of each community and trainer. Therefore, our planning topics and their respective class implementation methodologies are based on the studies and results found by the Data Goyá Institute team. This does not exclude the possibility of using or complementing other methods in each community, council, or organization.

6.1 PLANNING

In the planning stage, the implementation/execution of the course was designed, which included two complementary components:

- **Online component** : it was structured to be carried out through the platform coursetejiendoseguridad-digital.com , with six self-paced modules covering the fundamentals of digital security, common risks, and protection strategies. This phase allows instructors to familiarize themselves with and study the content at their own pace, accessing interactive materials, readings, practical exercises, and downloadable resources. Additionally, for those unable to attend the in-person activity, there will be an opportunity to access the content in two live online meetings.
- **In-person component** : Designed with an intensive and participatory approach, the course was designed to reinforce practical experience, generate collaborative dynamics, and consolidate the network of trainers. The one-day agenda includes welcome sessions, icebreakers, presentation sessions, and, above all, practical activities with templates, simulation exercises, and the use of digital tools. An active and participatory methodology is prioritized, with each theoretical session followed by a practical exercise to reinforce learning.

6.2 EXECUTION OF ONLINE TRAINING

During the weeks leading up to the in-person meeting, participants have the opportunity to access the online training. This allows them to:

- Acquire basic knowledge of digital threats, incident management, and data protection.
- Explore case studies and simulated scenarios of digital insecurity.
- Familiarize yourself with resources such as the **risk and solution canvas** and rapid response guides for digital attacks.

This way, by the time the in-person meeting arrives, the trainers will already have a common conceptual framework. And for those unable to attend the in-person meeting, a two-class live online session was developed so that the content of the in-person activity could also be shared with those participants.

6.2.1 The online course

The site appears as a proposed course aimed at Indigenous and Afro-descendant communities, with the goal of training leaders (or "digital guardians") so their community can navigate, participate, and protect itself in the digital environment. The sections visible in the menu are:

- Start
- Module 1: Our Digital Territory – Understanding the Internet Ecosystem
- Module 2: Our Rights in the Digital World
- Module 3: Caring for Our Digital Maloca – Community Cybersecurity
- Module 4: La Minga / Cabildo Digital – Internet Governance and Participation
- Module 5: Weaving Care Networks – Incident Response Protocols
- Module 6: The Role of the Community Trainer: Facilitating Knowledge

Upon [2]entering, the home page displays the title "TRAINING: WEAVING DIGITAL SECURITY" and a section titled "1. Purpose and Philosophy of the Course," which explains that the course is designed to train leaders of ethnic communities in Colombia as "Digital Guardians." It mentions that it is not a traditional technical manual, but rather a pedagogical approach aimed at empowering communities.

Next comes the section "2. The Pedagogical Approach: Hybridizing Training of Trainers with Popular Education." This section describes how to combine the Training of Trainers (TTT) model with the principles of Popular Education (PE). It details principles such as "Starting from Reality," "Dialogue of Knowledge," "Praxis (action-reflection-action)," and "Political Dimension."

Next, you'll see "3 Context: The Digital Reality of Ethnic Communities in Colombia." This section outlines the challenges: the access gap, the appropriation gap (skills, usage), threats in the digital environment (phishing, cyberbullying, exposure to risks), and suggests that connecting isn't enough, but also supporting training. Below is a support document with references for developing course materials.

[2]GOYÁ DATA INSTITUTE. *Welcome to the course Weaving Digital Security* [video]. YouTube, September 2, 2025. Available at: https://www.youtube.com/watch?v=e2SPEsiMqBQ . Accessed: Oct. 1, 2025.

6.2.2 Module 1: Our Digital Territory - Understanding the Internet Ecosystem

This module seeks to demystify technology and build a basic and critical understanding of how the Internet works, who manages or regulates it, and how the Internet relates to physical and community territory.[3] The module is divided into several classes, each with accessible theoretical explanations using analogies, plus practical activities to help participants ground the concepts in their reality.

The content is divided into three classes, with YouTube videos embedded on the platform/website. Class 1, [4]on the Internet from the abstract to the concrete, explains the physical infrastructure (submarine cables, fiber optics, satellites, antennas), and explains the Internet using a territorial analogy (rivers, roads, oral networks) to make the technical elements more understandable. The proposed practical activity was "Mapping Our Digital Territory," according to the curriculum.

Class 2 [5]addresses the issue of who rules the Internet, exploring the actors and power within the digital ecosystem. The *multi-stakeholder model* of Internet governance is presented, with stakeholders including the government, the private sector, academia, civil society, and the technical community. The practical activity proposed was the "Governance Table Role Play."

Class 3 [6]is about information flow, explaining where it comes from and where it goes. Basic technical concepts are explained using analogies: servers and the cloud, IP addresses, and data packets. The concentration of services and infrastructure in large corporations is discussed, along with the implications for diversity, data control, and digital sovereignty. The practical activity for this class is "The Path of a Message."

---

[3] Weaving Digital Security. Module 1: Our Digital Territory – Understanding the Internet Ecosystem. Google Sites. Available at: https://sites.google.com/view/tejiendoseguridaddigital/m%C3%B3dulo-1-nuestro-territorio-digital-comprendiendo-el-ecosistema-de-inter?authuser=0 Accessed: September 30, 2025

[4] INSTITUTO DATA GOYA. Lecture 1 of Module 1 - Our Digital Territory - Understanding the Internet Ecosystem. Published by: Instituto Data Goya, September 1, 2025. 1 video. Available at: https://www.youtube.com/watch?v=JiDd3-wIjzc . Accessed October 24, 2024.

[5]INSTITUTO DATA GOYA. Class 2 of Module 1 - Who Rules the Internet? Actors and Power in the Digital Ecosystem. Published by: Instituto Data Goya, September 2, 2025. 1 video. Available at: https://www.youtube.com/watch?v=l4WK6kj3XME . Accessed October 24, 2024.

[6]INSTITUTO DATA GOYA. CLASS 3 of Module 1 - The Flow of Information: Where Does It Come From and Where Does It Go? Published by: Instituto Data Goya, September 2, 2025. 1 video. Available at: https://www.youtube.com/watch?v=lc7ckp83fH0 . Accessed October 24, 2024.

The module understands the Internet not only as an external tool to be "used," but as a new digital territory that must be governed, defended, and appropriated by the community, in dialogue with its territorial and cultural values. It emphasizes that historical conflicts over land, power, and resources are replicated in the digital world: "data extractivism," disputes over the radio spectrum, the imposition of infrastructure that disrespects sacred territories, etc. A symbolic translation is proposed: cybersecurity can be seen as a "digital indigenous guardian," and internet governance as the construction of a "digital life plan" that dialogues with the community life plan.

The materials and assessment available for this module are: 1. A visible resource: "The Internet and its Governance." A PDF document appears as downloadable material for that module. There is also a test for Module 1 indicated.

Module 1 Exam - Our Digital Territory - Understanding the Internet Ecosystem * Indicates a required question
1- Full name * 2- Whatsapp * 3- Email *
4- How would you define “digital territory” based on what you have learned in this module? * Possible/expected response model: It is the virtual space in which communities interact, where information, culture and knowledge circulate, and which must also be protected as part of the community territory.
5- What is the importance of Internet Governance for our communities? * a- It doesn't matter b- If they make decisions that can change our digital reality, that's why we have to be included. c- It is an important space to impose legal procedures in digital matters Possible/expected response model: B
6- Why can the Internet infrastructure be compared to a river? * (If you wish, share photos of the practical activities carried out based on the topics proposed in this module.) Possible/expected response model: The internet infrastructure can be compared to a river because, like water, data constantly flows through different channels and branches. Just as a

river connects territories, councils, and ecosystems, the internet connects communities, devices, and people. Furthermore, any obstacle or contamination in the riverbed affects the flow of all those who depend on it, in the same way that an interruption or attack on the internet infrastructure impacts those who use it .
7- Do you have any suggestions, comments, or questions about this module? *
8- I authorize the processing of the information provided here exclusively for purposes related to the Weaving Digital Security course, in accordance with Law 1581/2012 and related regulations. I understand that I may withdraw at any time. *

6.2.3 Module 2 – Our Rights in the Digital World

This module translates the abstract framework of digital rights into concrete and defensible situations, empowering participants to recognize when those rights are violated and demand safeguards, both from digital platforms and the state. Lecture 1 [7]discusses human rights as a natural extension of digital rights.

The idea is raised that digital rights are not new, independent rights, but rather an extension of traditional human rights (privacy, freedom of expression, non-discrimination, access to information) to the digital realm. A review of the Colombian legal framework is undertaken, including Law 1581 of 2012 on personal data protection, as well as jurisprudence from the Constitutional Court that adapts these rights to the digital environment. The proposed practical activity is the "Word Circle."

In Class 2, [8]on the "Digital Rights Translation Matrix," a pedagogical table or matrix is introduced that serves to "translate" digital rights (legal concepts) into practical language, with everyday examples linked to the community context. Through this "translation," specific rights are explored. In Class 3, [9]on rights defense, mechanisms and

[7] **GOYÁ DATA INSTITUTE.** Module 2, Class 1 – From Human Rights to Digital Rights: A Natural Extension [video]. YouTube, September 2, 2025. Available at: https://www.youtube.com/watch?v=FYSBuTMxwP8 . Accessed on: October 1, 2025.

[8] **GOYÁ DATA INSTITUTE.** Module 2, Class 2 – Digital Rights Translation Matrix [video]. YouTube, September 2, 2025. Available at: https://www.youtube.com/watch?v=gbA8Rn1CeWQ . Accessed on: October 1, 2025.

[9] **DATA GOYÁ INSTITUTE.** Class 3 of Module 2 – Defending Our Rights: Mechanisms and Allies [video]. YouTube, September 2, 2025. Available at: https://www.youtube.com/watch?v=8QUfQvK_H9g . Accessed on: October 1, 2025.

allies are discussed, and practical ways to defend violated digital rights are explored. The proposed practical activity is the "Complaint Simulation."

The available materials include a PDF titled "LEGAL MAPPING – Assessing Current Digital Security Infrastructure, Practices, and Policies," as well as a presentation titled "Copy of Module 2 – Our Rights in the Digital World.pdf." There is also a quiz for the module, as shown below.

Module 2 - Our Rights in the Digital World * Indicates a required question
1- Full name * 2- Whatsapp * 3- Email *
4- Name three fundamental rights that apply to the digital environment and that were discussed in the module. * Possible/expected response template: Right to Privacy and Protection of Personal Data (Law 1581); Right to Freedom of Expression; Right to Identity and Own Culture; Right to the Protection of Children and Adolescents on the Internet
5- When analyzing digital rights, we can consider that some groups experience more violations. In your CSO, do you consider that women, men, or people with diverse gender identities face different digital risks? * A- yes b- No c- I don't know Possible/expected answer template: (This question doesn't have a single correct answer. Simply identify whether, from your perspective on digital rights, you can say that gender-related violations exist.)
6- How to address and resolve a digital rights violation situation? Possible/expected response model: In the event of a digital rights violation, the first step is to clearly identify the type of violation (for example, data theft, censorship, improper surveillance, unauthorized dissemination of information). Next, it's important to document the evidence (screenshots, emails, links) to prove what happened. It's necessary to inform the responsible platforms. In addition, you should inform and activate support networks: the community, digital rights organizations, or competent legal bodies. Depending on the severity, you can file complaints with authorities or seek

specialized legal advice. Finally, it's key to implement preventive and collective care measures to prevent the situation from recurring, such as improving passwords, implementing encryption, reviewing community protocols, and strengthening digital education.
7- *Informational self-determination* is the right of individuals and communities to decide how, when, and for what purpose their personal and collective data are used, ensuring control and consent over that information. In this context, how can we define *data sovereignty* ? a- The possibility for technology companies to freely use data to innovate. b- The autonomous control of peoples, communities and States over the collection, storage, access and use of their data. c- The right of governments to centralize all citizen data. d- Complete disconnection from the Internet to avoid misuse of information. Possible/expected response model: B - Data sovereignty can be understood as the capacity of peoples, communities, and states to exercise autonomous control over the collection, storage, access, and use of their data. Within the framework of informational self-determination, it involves not only protecting privacy but also ensuring that data—including community, cultural, and genetic data—are managed according to individual decisions, respecting identities, collective rights, and forms of local governance. We are sovereign over our data and information.
8- Do you have any suggestions, comments, or questions about this module? *
9- I authorize the processing of the information provided here exclusively for purposes related to the Weaving Digital Security course, in accordance with Law 1581/2012 and related regulations. I understand that I may withdraw at any time.

6.2.4 Module 3 – Caring for Our Digital Maloca: Community Cybersecurity

This module addresses cybersecurity from a community perspective, understood not only as a set of technical practices, but as part of the collective care needed to protect communities in the digital environment. It starts with the metaphor of the maloca, a traditional space for meeting and protection, and transfers it to the digital realm to reflect on how to collectively strengthen security.

In Class 1, [10]the most common digital risks facing communities are introduced, such as information theft, device attacks, and online spying, and basic prevention strategies are discussed. The proposed practical activity is a "Community Digital Risk Mapping" exercise, in which participants identify specific threats in their own context.

Class 2 [11]teaches fundamental security practices in a simple, memorable, and immediately applicable way. It focuses on the use of digital security tools, exploring encryption practices, secure password management, backups, and mobile device configuration. The goal is for participants to be able to apply concrete measures in their daily lives. The class includes a step-by-step, guided "Secure Configuration Workshop."

Classes 3 [12]and 4 [13]delve deeper into the collective dimension of cybersecurity, highlighting the importance of creating community protocols for care and response to digital incidents. A curated catalog of digital tools is presented that are open source (allowing auditing and generating greater trust), free, and, crucially, designed to function 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.

It also reflects on how solidarity and organization strengthen shared protection. The proposed practice is the construction of a "Community Response Protocol" tailored to the circumstances of each group. The available materials include a PDF document titled "Basic Community Cybersecurity Guide," along with supporting presentations and sample protocols. A module quiz is also included at the bottom of the page.

Module 3 - Caring for Our Digital Maloca - Community Cybersecurity * Indicates a required question

[10] **DATA GOYÁ INSTITUTE.** Module 3, Class 1 – Community Risk Map: What Are We Protecting Ourselves From? [video]. YouTube, September 1, 2025. Available at: https://www.youtube.com/watch?v=VHGfxfkzgBA . Accessed on: October 1, 2025.

[11]GOYÁ DATA INSTITUTE. *Class 2 of Module 3 - Basic Digital Hygiene and Care: Our First Steps* [video]. YouTube, September 1, 2025. Available at: https://www.youtube.com/watch?v=l6CDPhpbiLg . Accessed: Oct. 1, 2025.

[12] **DATA GOYÁ INSTITUTE.** Module 3, Class 1 – Community Risk Map: What Are We Protecting Ourselves From? [video]. YouTube, September 1, 2025. Available at: https://www.youtube.com/watch?v=VHGfxfkzgBA . Accessed on: October 1, 2025.

[13]GOYÁ DATA INSTITUTE. *Module 3, Class 4 - Digital Care Tools Catalog* [video]. YouTube, September 1, 2025. Available at: https://www.youtube.com/watch?v=Lr7H5bZ7RBU . Accessed: Oct. 1, 2025.

1- Full name * 2- Whatsapp * 3- Email *
4- What does "Maloca Digital" mean in this module? And what are the main recommended community cybersecurity practices? * Possible/expected response model: A digital maloca is a community digital space, equivalent to a physical maloca, that must be protected and cared for collectively. The following are recommended for this space: Use of secure passwords, backups, software updates, digital education, and collective care protocols.
5- Have you or anyone in your community/organization experienced harassment, threats, or digital violence related to your gender or sexual orientation? * A- Yes b- No c- I don't know Possible/expected response template: This question doesn't have a single correct answer. Simply identify, from your perspective on cybersecurity, whether your community/organization has previously experienced threats or digital violence based on gender or sexual orientation.
6- Imagine you're traveling and need to connect to a public Wi-Fi network at a café. You want to protect your information and prevent anyone from spying on your connection. Which of these tools would be most appropriate in that situation ? a- Signal, for secure chatting. b- KeePassXC, to save your passwords. c- ProtonVPN, to encrypt and protect your connection on the public network. d- Cryptomator, to store documents in a secure vault. Possible/expected response model: C - In the event of a risk of interception on public WiFi, the indicated tool is ProtonVPN, because it encrypts the entire connection, while the others protect different aspects (messages, passwords or files).
7- Do you have any suggestions, comments, or questions about this module? *
8- I authorize the processing of the information provided here exclusively for purposes related to the Weaving Digital Security course, in accordance with Law 1581/2012 and related regulations. I understand that I may withdraw at any time.

6.2.5 Module 4 – The Minga/Cabildo (Council) Digital: Internet Governance and Participation

This module addresses the idea of the minga/ cabildo or council as traditional spaces for collective deliberation in Indigenous communities, and how these forms of organization can interact with contemporary models of Internet governance. It begins with a reflection on what digital governance means and why it is essential for communities to be not only users but also active participants in decision-making about the future of the Internet.

Class 1 [14]introduces the principles of Internet governance, demonstrating its multi-stakeholder and multi-level nature, and explains how decisions made by international organizations directly affect local communities. Class 2 [15]focuses on the relationship between the minga/cabildo (council) and digital participation spaces, highlighting the importance of bringing community values such as collective action, consensus, and mutual care to the digital environment.

Class 3 [16]addresses examples of participation in Internet governance forums, from local to global levels, and explains how communities can influence these processes. As a practical activity, we propose a "Digital Minga Simulation," in which participants recreate an online collective deliberation space to discuss a topic related to digital rights and community security. The available materials include a PDF presentation, a guide for trainers, a sample digital minutes, and a module-ending exam.

Module 4 - La Minga/Cabildo Digital - Internet Governance and Community Participation * Indicates a required question
1- Full name * 2- Whatsapp * 3- Email *

[14]DATA GOYÁ INSTITUTE. *Lecture 1 of Module 4 - What is Internet Governance and Why Do We Care?* [video]. YouTube, September 3, 2025. Available at: https://www.youtube.com/watch?v=HpQlgyCJL6s . Accessed: Oct. 1, 2025.
[15]DATA GOYÁ INSTITUTE. *Lecture 2 of Module 4 - The Colombian Internet Governance Roundtable: A Space for Influence* [video]. YouTube, September 3, 2025. Available at: https://www.youtube.com/watch?v=u2cy65vUqRY . Accessed: Oct. 1, 2025.
[16]DATA GOYÁ INSTITUTE. *Class 3 of Module 4 - Building Our Agenda: From Complaint to Proposal* [video]. YouTube, September 3, 2025. Available at: https://www.youtube.com/watch?v=zw6XkXx0ZH0 . Accessed: Oct. 1, 2025.

4- How can Internet governance strengthen autonomy and community organization? * Possible/expected response model: Ensuring participation in decisions about the use of technologies, promoting inclusive access, and defending collective digital rights.
5-How would a digital assembly work in your community based on what you have learned? * Possible/expected response model: Use of secure platforms, community moderation, digitally recorded collective decisions.
6- What is the main purpose of the Cabildo (Council) *Digital Act* in the communities? * a- Register community agreements on connectivity, data protection and cultural use of platforms. b- Save community leaders' passwords in a single document. c- Collect evidence on individual cybersecurity incidents. d- Centralize community information under the exclusive control of the State. Possible/expected response model: A - The Cabildo (Council) Digital Act is a symbolic and practical tool that communities use to put in writing their collective agreements on how they want to inhabit and govern the digital territory. According to the module guide, this document documents community decisions regarding: Connectivity (e.g., requiring community networks or differentiated rates); Data protection (consent protocols, protection of sensitive information); Cultural use of platforms (how songs, textiles, dances, or other knowledge are shared without risk of misappropriation); and Prior consultation protocols in the digital sphere. Therefore, the correct option is a) Register community agreements on connectivity, data protection and cultural use of platforms, as it faithfully reflects the purpose of the Cabildo (Council)Digital Act.
7- Do you have any suggestions, comments, or questions about this module? *
8- I authorize the processing of the information provided here exclusively for purposes related to the Weaving Digital Security course, in accordance with Law 1581/2012 and related regulations. I understand that I may withdraw at any time.

6.2.6 Module 5 – Weaving Care Networks: Incident Response Protocols

This module explores community strategies for creating care networks and digital incident response protocols. The central premise is that digital security should not be thought

of solely in technical or individual terms, but rather as a shared responsibility, sustained by trust and mutual support.

Class 1 [17]introduces the concept of care networks, showing how they are built within communities and how to translate these practices into the digital environment. Class 2 [18]addresses what a digital incident is, the different types that can occur (attacks, data breaches, online harassment, etc.), and how to address them collectively.

Class 3 [19]is a practical class and focuses on designing response protocols, exploring practical tools to enable a community to react quickly and in a coordinated manner to a digital risk. The practical activity consists of creating a "Care Network Map," in which each participant identifies actors, contacts, resources, and support pathways that can be activated in the event of an incident. Module materials include a PDF presentation on the content, an incident template document, and a closing exam to assess what has been learned.

Module 5 - Weaving Care Networks - Incident Response Protocols * Indicates a required question
1- Full name * 2- Whatsapp * 3- Email *
4- What is meant by “care networks” in the digital context? * Possible/expected response model: Collective support and solidarity strategies to address digital risks in a community manner.
5- What basic steps should a community digital incident response protocol include? * Possible/expected response model: Incident identification, clear communication, risk mitigation, logging and tracking.
6- If a person in the community receives a suspicious *phishing email* , what would be the most appropriate initial action according to the Community Rapid Response Protocol? * a- Ignore the message and do nothing.

[17]DATA GOYÁ INSTITUTE. *Lecture 1 of Module 5 - Care Networks* [video]. YouTube, September 1, 2025. Available at: https://www.youtube.com/watch?v=VS6gUUKS48c . Accessed: Oct. 1, 2025.
[18]DATA GOYÁ INSTITUTE. *Module 5, Class 2 - The 5 Steps of the Incident Protocol* [video]. YouTube, September 1, 2025. Available at: https://www.youtube.com/watch?v=V5AS-OhK5rU . Accessed: Oct. 1, 2025.
[19]DATA GOYÁ INSTITUTE. *Practical class for module 5 - Protocol Template (Creating Our Own Community Protocol)* [video]. YouTube, September 1, 2025. Available at: https://www.youtube.com/watch?v=hLnctburnxQ . Accessed: Oct. 1, 2025.

b- Inform the affected person, disconnect the equipment from the Internet and change the main password. c- Reply to the suspicious email to confirm if it is real. d- Post the email on social networks to alert without further verification. Possible/expected response model: B - Phishing is a deceptive attempt to steal sensitive information, such as passwords or banking details. According to Step 1: Contain in the Community Protocol Template, the community must act immediately to prevent the attack from spreading or causing further damage. The initial actions are: Notify the affected person so they are aware of the risk. Disconnect the device from the internet, cutting off any possible external access. Change the master password, preventing the attacker from further using the information. In this way, the individual and the community are protected, reducing the impact of the attack before moving on to the next steps of the protocol (document, communicate, act, and learn).
7- In your community/organization, do you have a psychosocial or legal support channel for situations where there are victims of gender-based violence/discrimination based on race or ethnicity facilitated by technology? * A- No b- Yes Possible/expected response template: This question doesn't have a single correct answer. Simply identify, from your perspective on cybersecurity, whether technology-enabled support channels for victims of violence already exist in your community/organization.
8- If you answered yes to the previous question, could you tell us what type of support channel it is? Possible/expected answer model: This question does not have a single correct answer.
9- Do you have any suggestions, comments, or questions about this module? *
10- I authorize the processing of the information provided here exclusively for purposes related to the Weaving Digital Security course, in accordance with Law 1581/2012 and related regulations. I understand that I may withdraw at any time.

6.2.7 Module 6 – The Role of the Community Trainer : Facilitating Knowledge

The final module is dedicated to those who will assume the role of trainers in their communities, in order to ensure the replication and sustainability of the knowledge acquired

in the course. Class 1 discusses the Art of Facilitating, introduces the role of the community trainer, and outlines pedagogical principles for popular education and adult training, highlighting the importance of drawing on communities' own knowledge and promoting participatory methodologies.

Class 2 is replication planning, from idea to training action, approaching a model plan to implement training in a few steps:

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 important 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 will 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.

Class 3 focuses on the Trainer's Toolbox, presenting a set of practical facilitation resources and techniques. The proposed practical activity is the "Workshop Simulation," in which participants prepare and facilitate a short session based on the course content, receiving feedback from the group. This module concludes the activities; it does not include audiovisual materials, and the final exam assesses participants' overall perception of the online course.

Module 6 - The Role of the Community Trainer: Facilitating Knowledge * Indicates a required question
1- Full name *

2- Whatsapp * 3- Email *
4- How do you intend to implement the learnings from this course as a community trainer/facilitator? *
5- Do you think you can apply the knowledge acquired in the course in practice in your daily community life? * No Yeah Other:
6- Do you have any suggestions on a topic that should be included in the course? *
7- How would you rate your satisfaction with the course on a scale of 1 to 5? * (1 being dissatisfied and 5 being very satisfied)
8- Do you have any suggestions, comments or questions? *
9- I authorize the processing of the information provided here exclusively for purposes related to the Weaving Digital Security course, in accordance with Law 1581/2012 and related regulations. I understand that I may withdraw at any time.

6.3. EXECUTION OF FACE-TO-FACE TRAINING

The in-person meeting will consolidate the process through an intensive day of collaborative work. The planned agenda includes:

- **Opening sessions** : accreditation, welcome, and icebreakers to strengthen group trust.
- **Content block** : short presentations on digital governance, digital rights, digital sovereignty, and security tools.
- **Practical activities** : the Rights, Violations, and Solutions Canvas, where participants identified specific digital security issues and proposed alternatives; the Digital Record, as an exercise in recording and documenting risks; the Use of Apps and Tools, with guided activities to experiment with technological solutions; and the Incident Template, focused on response protocols for digital attacks.

- **Closing and feedback** : time for questions, comments, and final reflections, followed by a moment of informal socializing.

6.4 EXPECTED RESULTS

The combination of the two components (online and in-person) will ensure that trainers have a solid conceptual foundation in digital security topics. At the same time, the combination of in-person and online training will allow them to develop the practical skills needed to apply and teach what they have learned.

In addition, the course will facilitate the generation of shared materials and templates ready for replication. The main expected outcome is a strengthening of the sense of community and network among trainers on the topic of digital security, creating a space of trust and collaboration.

7. EVALUATION AND MONITORING

The assessment will be conducted at different levels: I- **Initial assessment (baseline):** assessment of participants' prior knowledge and expectations; II- **Continuous assessment:** feedback via the WhatsApp group, individually for each module, to measure the course's usability, accessibility, and practical application; III- **Final and impact assessment:** assessment of acquired skills and content understanding through analysis of completed activities/forms.

REFERENCES

MACHADO LEAL, Denise; ROJAS MARCELO, José A.; VELASQUEZ, Umut Pajaro. Digital security assessment: information for strategies to strengthen the digital capacity of indigenous and Afro-descendant organizations, communities, and peoples in Colombia. Critical review: José A. Rojas Marcelo. Content review: Umut Pajaro Velásquez. Ethnic perspective review: Suya Corridor. Style design and editing: Denise Machado Leal. Rubiataba, GO: Data Goyá Institute, 2025.

VELASQUEZ, Unnut Pajaro; MACHADO LEAL, Denise; ROJAS MARCELO, José A. Community digital guardians: a training of trainers curriculum in cybersecurity, governance, and digital rights for indigenous and Afro-descendant communities in Colombia. Content review: Unnut Pajaro Velásquez. Ethnic perspective review: Suya Corridor. Edited and styled by Denise Machado Leal. Rubiataba, GO: Data Goyá Institute, 2025