REPORT

Digital security organizations in Latin America

APRIL 2024

American Friends Service Committee

Table of contents

Sursiendo team: Domingo M. Lechón & Candy Rodríguez

San Cristóbal de Las Casas, Chiapas.

Introduction

Throughout the last few years, civil society organizations in Latin America have conducted research or training processes related to digital security with a greater consistency and scope. This is the area where this research is focused.

Digital rights organizations in Latin America have played a crucial role in the promotion of digital security in the region. These organizations have managed to achieve significant progress in creating awareness about the importance of protecting online privacy and liberties, as well as in the implementation of tools and strategies to guarantee the security of all users within a digital environment. Nevertheless, these achievements have faced their fair dose of substantial challenges, such as the evolution of digital attacks, the criminalization of the defense of digital rights, espionage held by public institutions, the promotion of laws that violate digital rights, the lack of resources to perform their activities, as well as the need for constant updates, among others, and which required continued assistance and a strategic focus. The focal point here is filled with thoughts and analysis that the organizations make, and which they then share with the rest of society in the shape of resources and materials.

To be able to have a broader landscape of what digital security looks like in Latin America, it was decided to collect contributions from the organizations in the whole region. These groups work some aspects of digital security and may be considered as defenders of digital rights, given they address digital security as part of comprehensive security, or from a standpoint of *hacker* fights, free culture or freedom of speech.

These very diverse organizations are also part of broader, regional, networks and links, which allows them a greater reach and continuity. The main reason to conduct research from a regional perspective is highlighted by the Latin American context itself, where there are common origins, the same language is spoken in the large majority of countries, there are similar electoral processes taking place, similar punitive legislative currents, a perceivable increase on the attacks of freedom of speech throughout the whole region, multiple shady laws which have attempted to hurt other human rights allegedly on behalf of the victims; as well as a direct attack against social mobilization, a greater number of feminicides, digital attacks due to gender issues, the increase of migration flows, the permanence of extractivism, and last but not least economic, cultural and digital colonialism.

The overall presence of social movements resisting capitalism, violence and colonialism in digital spaces, as well as the use of up to date technological tools has seen an increase, and as such, digital security has been included for a few years now in all social agendas and movements.

Literature review

A multitude of research related to digital security in the region has been conducted from the academic world, usually addressing these issues from a standpoint of "cybersecurity and cyber defense". However, we would like for our focus to be on the digital security related to journalism, activism and organized civil society defending human rights.

In this environment, meaning that of social organizations, productions have been conducted related to digital security and mainly focused on practical experiences or in support of said trainings, however, these reports and analysis have also been produced concerning digital gaps, public policies, corporate abuse, social innovation, gender violence within digital spaces, and human rights violations, amongst other issues.

As an example, which would serve as a great starting point we have ***Libertades en retroceso, Entre el autoritarismo y la defensa de la democracia en América Latina***[1] ***(Shrinking freedoms, Caught between authoritarianism and the defense for democracy in Latin America)***, a report drafted during 2023 by Espacio Público para la Alianza Regional por la Libre Expresión e Información (Public Space towards a Regional Alliance for Free Expression and Information); which highlights the importance of digital space, where there is a "deterioration of the public debate resulting in specific consequences within the civic space and enjoyment of human rights", and that after taking a close look at 13 countries in the region, concluded that "the abuse of power is the common axis in countries experiencing severe human rights violations or attacks to democratic institutionality".

Another good example is the report ***Remoción de contenidos: Desigualdad y exclusión del espacio cívico digital***[2] ***(Removing content: Inequality and exclusión within the digital civic space)***, from 2021. In this report, the organization Article 19, Mexico and Central American Office, meant to "render an account of how removing content perpetuates and empowers different forms of discrimination and social exclusion in Mexico" and also "analyzes how content removal or elimination practices have a specific impact on the identities or causes that people vindicate, visibilize, defend and/or promote".

We may also highlight the contributions of the regional coordination Internet Ciudadana[3] (Citizens Internet), which has been jointly working to build a perspective from the Global South about digital technologies through convergence from the level of local grassroot organizations concerned by digital technologies. Internet Ciudadana has held multiple meetings, forums and has disseminated materials with a critical focus, where the different digital breaches are analyzed, along with the dangers presented by corporations and

1 *https://www.alianzaregional.net/coleccion-articulo-xiii-libertades-en-retroceso-entre-el-autoritarismo-y-la-defensa-de-la-democracia-en-america-latina/*
2 https://articulo19.org/informe-remocion-de-contenidos/
3 https://al.internetsocialforum.net/

legislations, while also promoting the use of free tools and the existence of alternatives, "to build common agendas towards the internet of the people".

In other Latin American articulations and links related to digital security we can highlight the contributions of the Asociación para el Progreso de las Telecomunicaciones[4] (Association for Progress in Telecommunications) (APC), COSIC.lat[5] or the consorcio Al Sur[6] (Al Sur consortium), all of which are made up of Latin American civil society organizations that defend digital rights and promote the ethical and free use of digital technologies.

Organizations that focus on digital security processes usually have sections on their websites where they publish references, reports or resources, which go beyond tutorials on tools or apps but also social recommendations or political analysis and forms of action.

In the Blog section of SocialTic, Mexico[7], we are offered a large amount of resources, such as the "Launch of Datavoros: Discover how much the apps you use, feed from you" or "Girs and IT: digital security and privacy", that go into greater technical analysis, but mostly, proceed to assign technologies a place within each social and political context, highlighting feminist positions.

In the Publications section of the Hiperderecho[8] web, in Perú, there is a contribution on "Digital protection during protests", a "Guideline to protect and present evidence in cases of online gender violence" or "ACuerpándonos for a feminist, diverse and free internet", meaning, going from very basic issues to proposals for the social analysis of technologies.

In the resources section of Fundación Acceso[9], which is an organization that operates throughout Central America, we are shared infographics, videos, articles and publications related to "the contribution to strengthen organizational capacities", promoting "digital security and comprehensive protection for organizations and people that work defending human rights".

In the Mexican web Técnicas Rudas[10] there is a section on Resources, where they share practical tutorials, technology comparison tables, or technopolitical context analysis. Just like with our blog in Sursiendo[11], we have texts on thoughts pertaining sociotechnical processes, such as the *Digital Watch in Mexico*[12], along with a guideline of tools, platforms or safer processes.

These examples illustrate the fact that there is a broad bibliography being shared by the organized Latin American civil society, where they collect issues pertaining freedom of speech violations, ways to protect themselves, violence towards women, the promotion of cyber-

4 *https://www.apc.org/es/publications*
5 *https://cosic.lat/*
6 *https://www.alsur.lat/reportes*
7 *https://socialtic.org/blog/*
8 *https://hiperderecho.org/publicaciones/*
9 https://www.acceso.or.cr/
10 *https://tecnicasrudas.org/es/recursos*
11 *https://sursiendo.org/*
12 https://sursiendo.org/2019/05/vigilancia-digital-en-mexico/

feminist activities, digital care as a collective practice, and digital autonomy facing digital colonialism, all of which promote threats and (digital) rights violations, breaking with digital gaps caused by the lack of possibilities to access technology or due to the lack of training to use said technology, as well as going beyond the technical aspects to build security with a comprehensive focus in moments of generalized violence as well as a world focused on all things digital.

Research design and methodology

In mid-July, Sursiendo's participation in the American Friends Service Committee (AFSC) research proposal for the Latin American region was confirmed; and at the end of the month, Sursiendo's research team, made up by a two person team with ample experience in research on socio-technical processes, digital rights and security, was formed.

To begin, we established a work plan based on a research timeline and determined the research techniques and methodological tools we would be using in regard to the objectives of the research. Thus, we focused mainly on understanding how civil society organizations in the region are creating tools, curricula, training and educational processes to deal with digital attacks from different perspectives in digital security.

The research includes the following points:

- Concise and detailed literature review on this topic of digital security as of January 2018.
- Recent incidents suffered by civil society actors who have been targeted in relation to digital security and safety.
- Key regional challenges related to this thematic area.
- Governments or state authorities that respect or defy cyber laws.
- National and international organizations and networks currently responding to this issue and in what ways.
- Existence of tools, training, resources or strategies in the region to protect the secure transfer of information.
- How these tools are or are not accessed.

To carry out this work we established a ***first phase*** to begin mapping social organizations, as well as materials, resources or tools, clearly linked to digital security, to then move on to the ***second phase***, which consisted in drafting a questionnaire meant for organizations, which would allow going into a ***third phase*** which included the selection, contact and forwarding of the interview to at least 15 organizations in the region. The final round was the ***fourth phase***, which entailed the collection of information provided by the informants as well as the documentation reviewed, analyzed and systematized to be able to draft this report.

To select the organizations which would be chosen to be included in the mapping, we prepared a list of all the ones we knew from all the years of experience in the field work with social organizations. Most assuredly, we left a few of them out, however, we were able to map

fifty one total, as seen in Annex 1, thirty nine organizations and collectives with presence in thirteen countries of the region, as well as twelve projects o alliances at a regional level that work with these issues.

And for the choice of who we would send the questionnaire to in order to make it a meaningful sample, we thought of some who had recognized work in digital security training with civil society organizations, who participated in networks or articulations and who we believed could contribute to the objectives of this research.

Out of this search, we managed to interview nineteen organizations in Mexico, Chile, Brazil, Argentina, Ecuador, Costa Rica (working throughout all of Central America), Peru, Bolivia and Paraguay, managing to conduct a qualitative interview on their focal points when implementing digital security workshops, as well as the main challenges, achievements and materials they have developed over time to address digital security issues.

The methodology of the interviews was based on participatory action, which implies a process of exchange of knowledge and instances that allow learning from experience. The questions we asked for the interview were the following:-

What is the focus of the digital security workshops you teach: holistic, integrated security, human rights, or mental health issues? And why did you decide to use this approach?

What have been the main challenges you have identified in the digital security trainings/workshops?

What have been your main achievements in these workshops?

What tools or resources on digital safety have you published, or do you use?

Has your country promoted or approved legislation that threatens human rights in the digital space of defenders or society in general? Please provide details.

Due to the short time we had to develop the work, we decided to conduct the interviews through three digital tools, including e-mail, direct messaging applications (text or audio) and video calls. Of the nineteen interviews, five were via audio, two were video calls and twelve were via email.

Although we had a limited time of two weeks for the interview and document review process, which posed a challenge in terms of addressing relevant information, we obtained a good response from the organizations, despite the fact that most of the people we approached had very tight schedules, so some declined or were unable to provide us with their answers. Even so, we were able to sustain this research with relevant information.

Summary of results

Digital security in Latin America has found diverse approaches and formulas when being facilitated by collectives and civil society organizations. Through this summary we will be able to realize that each training and each organization has different approaches and methods that depend on the needs and contexts of the communities they work with.

Through the interviews we were able to determine that it is not the same working with women, gender diversity groups, land defenders, journalists, feminist collectives, students, community networks, indigenous groups, people with disabilities, corporations or governments; however, the majority of organizations share focal points and things in common, such as human rights, gender rights, technopolitical, legal, holistic, ,feminist or comprehensive security perspectives, and have taken into consideration popular education and decolonial methodologies.

The use of specific language, as well as the terms used to address digital security contain a political burden given they´re accompanied by discrepancies, perspectives and interests as established in the *Digital Security and Human rights: A perfect match* report, where it is stressed that when referring to digital security, this entails putting at "the center protecting people and, consequently, human rights", as opposed to cybersecurity - which is a term widely used in the media and social networks - and "consists of the preservation, through policies, technology and education, of the availability, confidentiality and integrity of information and its infrastructure" a more rigid vision, sometimes militarized and without a human rights perspective.

The organizations we interviewed focused on the use of language around how they name digital security and made reference to how the terms have changed over time and their experience.

- NGO Amaranta went from talking about *digital* self-care, to speaking about *digital community care*, understanding there is a prevailing “extractive and individualistic logic which has led us to believe that we are alone when we go online, without realizing that it is in fact a profoundly community based activity. NGO Amaranta
- Técnicas Rudas speaks of *digital care or feminist self-defense* which refers to one of the aspects of digital care.
- Vlta Activa addresses *holistic security* which considers the digital body and the physic/psychic body within comprehensive digital protection.

And this is how from so many different parts of the region, concepts are being used which adjust themselves to the communities and the different focuses belonging to each organization and territory.

Amongst the methodologies and focuses adopted by these organizations are the following:

- The socio-affective methodology involves talking to people from their experiences and manages to identify why digital security and digital rights are important for life.
- Learning as a horizontal and collective process that places the care of space, people and processes at the center.
- Methodologies that have been inspired by popular education and their activities are focused on digital care and their learning processes where they provide elements of physical, patrimonial and care security among activists.
- Methodology of feminist popular education where they prioritize the processes of individuals with the interest of creating horizontal spaces, starting from the fact that the facilitators do not know everything, but they can exchange knowledge and experiences together where they position themselves as facilitators and not as trainers - which makes a difference between teaching and sharing/constructing-.

On the other hand, there are also organizations that focus on games and enjoyment.

- Luchadoras, have a feminist perspective, more and prevention and focusing on the pleasures of navigating the Internet (not only the risks).
- For #SeguridadDigital it is important to think that digital care is something dynamic, sort of like a gradual process that takes place through games with dynamics that can be fun. They have held crypto parties, stickers, etc. The objective is to walk away from fear from a place of fun.

Other perspectives include the political and critical approach to technologies, which allow the development of capabilities and transformations that make it possible to reduce and mitigate these risks.

- From Sursiendo we have chosen (so long as it is possible) to use free and reliable technologies that allow us/them to live our "digital lives" in the long path towards technological autonomy.
- The collective 0xche understands collective understands digital security holistically and tries to critically question the use of technology, so they offer tools from the security field, such as threat modeling, so that people who are part of the workshops can make critical and informed decisions about their digital body.

Another focus adopted by different organizations is to provide trainings in different levels, such as the legal aspect and its link to technology.

- ARTICLE 19 provides a cross-cutting approach in its trainings where they seek to put people at the center and analyze what social categories may be intercepting them, such as: psychosocial, legal, legal, and digital.
- TEDIC offers workshops on digital security with a broader perspective: they include aspects of legal security and propose the debate on rights with a political, not only technological, approach.

- Hiperderecho provides comprehensive support (technological, social, legal and psychosocial) on an individual basis, based on the idea that each person has his or her own process and habits, and collectively identifies points in common and shares positive and non-positive experiences, as well as community practices.

The intent behind these projects is to spark conversations and share practices which may lead us to have a more conscious digital life, in which users, as individuals, may have a larger margin for decision making and be better informed so as to be able to make educated decisions, as mentioned by Comuna Digital.

Although the methodologies, approaches and forms are very similar among organizations, the challenges and communication gaps are also widened by socioeconomic factors that cross the entire region. This leads to inequalities in digital literacy processes.

One of the most important challenges is related to the territory, the digital divide and the poor connectivity that may exist in certain places. At Sursiendo we work with people from rural and urban areas, from different ethnic groups, and one of the elements that make it difficult to build a more robust accompaniment is that we find that there is no perception of all things digital as a vulnerability factor, so we focus our training on risk awareness.

TEDIC mentions that in Paraguay they have had similar processes when working with indigenous communities, they found that digital attacks were not a priority in their context, but instead to think about other things such as connectivity, the use of digital tools, the digital divide and therefore have sought to have multidisciplinary perspectives not only with technologists, but also with anthropologists who accompany them during these trainings. At the same time, they recognize that many times the organizations that provide this type of advice are not close to the territories, so there is a centralization and little access to information.

While inequality gaps are widening for these reasons, in Latin America there is a context of Government surveillance that has manifested itself mainly against human rights defenders, activists, journalists and civil society in general. The Mexican case has been one of the most famous to date, given the broad display of government institutions using Pegasus spyware, which has been active since at least 2012 and has continued operating to date, even in spite of the change in administration[13]. Pegasus has also been used in Honduras[14], Guatemala[15] and El Salvador[16], that we know of.

It is important to focus on the deployment of surveillance mechanisms in contexts such as those of Latin America, which are tending towards repressive and punitive policies in the digital environment, in order to silence, monitor and punish criticism and autonomy

13 https://elpais.com/mexico/2022-10-03/el-ejercito-mexicano-compro-en-2019-pegasus-para-espiar-a-activistas-y-periodistas.html
14 https://tiempo.hn/que-es-pegasus-espionaje/
15 https://nomada.gt/pais/la-corrupcion-no-es-normal/espionaje-ilegal-del-gobierno-aqui-esta-la-investigacion-de-nuestro-diario-parte-i/
16 https://www.lavanguardia.com/internacional/20230802/9146585/periodistas-el-salvador-espionaje-pegasus.html

processes. Therefore, we also find common in the region, legislative agendas contrary to the respect of human rights in digital contexts (Map in Annex 3).

Analysis, discussions and implications

As we saw in the previous section, the context and inequality gaps have widened due to various difficulties and considerations which have marked the objectives and modified the methods and techniques to carry out these activities.

Through the interviews, we were shared testimonies, considerations and difficulties the organizations were experiencing in very similar ways regardless of the country they were in.

On the one hand, time is a very important factor during these processes. Learning about digital security is a gradual process, and moves at its own time and considerations. A person does not become an expert just by participating in a workshop, they will always need time to become familiar with something and incorporate it into their daily individual and collective practices.

- Tierra Común mentions that for a digital security accompaniment to be good it needs to have a medium term period for questions to arise and also to allow time for a diagnosis and attention process.
- In Sursiendo, we believe that groups and organizations interested in improving their digital practices with a focus on security, generally pay attention and implement actions once they´ve been able to identify a risky situation or once they´ve suffered an attack.
- 0xche mentions that the challenge of introducing a topic without it seeming complex or unreachable is by only providing the necessary content so that activists are fully able to understand the types of threats they are exposed to, however that does not allow the creation of tools, preventive measures or action plans when faced with digital attacks.
- In this sense, ARTICLE 19 considers that it just may be too much information for a single workshop, and implementation can be stressful, which leads to an extenuating process which does not allow for continuity.

Social TIC mentions that to creating playful and innovative curricula becomes a challenge and the possibility of being didactic in order to help people understand technical concepts that are difficult to translate or explain in depth, and that is a challenge because it implies approaching a diversity of experiences, familiarization and feelings towards the digital world. The sensitization and awareness of what digital security implies goes beyond installing a program or changing some passwords, they are a constant challenge in a world where digital security does not seem to be an inherent part of digital literacy.

And, as a matter of fact, digital safety literacy processes facilitate understanding and break down stereotypes regarding people who use the Internet and digital tools. The Red Transfeminista de Ciudadanos Digitales (Transfeminist Network for Digital Care) mentions that among its greatest challenges, it has found that people believe that they cannot do it and that technology is for experts. Added to the prevailing lack of awareness and knowledge about digital risks.

- Fundación Acceso mentions that the lack of access to resources of various kinds and overall lack of knowledge about appropriate tools, plus the constant evolution of cyber threats are among its greatest risks. In addition, tailoring workshops to the specific needs of participants can be a challenge, especially when bringing together people with different training needs.
- Hiperderecho conducts surveys before every training and search for the differences between the habits and tools within a same group of persons, which can be quite varied, reason why trying to standardize the contents at the beginning is not the same.
- MariaLab mentions that the "way in which it is so easy to use internet platforms, and the fact that doing so is free, makes it easier for them to continue being used as the main means of communication and organization of activist groups and organizations". And this leads to a violation of other rights such as privacy, and the freedom to navigate on the Internet, and although we do agree with the opinion that there should not be a moralist vision attached on how digital tools are used, we cannot ignore how critical their use is.

Another factor to analyze is that there is a lack of knowledge regarding what behaviors constitute digital attacks because there are dimensions, due to gender issues, activism or simply attacks that are digital violence and not online gender violence. NGO Amaranta mentions that it is important to recognize online gender violence and its workshops are mainly focused on giving attention to it from this perspective and mentioning digital security with a feminist and human rights approach.

Monitoring something is complicated due to lack of time, as well as being up to date with all the technology #SeguridadDigital mentions that there is always that sense of being a little behind, technology moves so fast, and so do attack techniques, reason why it is hard to be constantly up to date, and in so little time.

Undoubtedly, technological progress and updating are relevant issues to be addressed because they not only involve updating community standards, but also tools, knowledge of digital attacks, forms of violence and the creation of methodologies that adapt to technological progress.

Técnicas Rudas also mentions something similar. And what they do is they stay up to date, however they feel said updating exceeds them, given they don´t have much funds and are an organization that makes their living from conducting workshops, and they feel its time consuming to do the research, study, learn new things, it takes a lot of work, and it overlaps with labor precariousness. And the latter is why the challenge of achieving work sustainability is a challenge that cannot be cast aside. The majority of organizations provide

trainings, accompaniments and study plans at solidarity prices or even free of cost, many times thanks to the funds providing by foreign donors. Técnicas Rudas has mentioned the importance of “changing certain logics and assume a perspective from the standpoint of a feminist economy”, or refrain from allowing the endangerment of those of us holding these activities. Digital security entails multiple individual and collective care for it to work, also the fact that specialization requires work.

Because of all of the above, it is also complex to know whether or not the workshops have a later impact on the people who take them: it is possible to see that there is an important level of awareness, however it is unknown if there are technical challenges when implementing tools and care strategies, and due to lack of time and follow-up, it cannot be attended.

Therefore, it is important to share specific guidelines or tools that can be useful after the workshop. Currently the age and intergenerational condition is important because the biases with the communities are very different. It goes to the importance of asking questions as an organization about the terms and languages we use.

And while updates, constant digital threats, job insecurity and cultural and social differences are not the only things that civil society organizations have faced. There is currently a wave of legislation and use of legal tools that have attempted to regulate issues related to digital rights and digital security or cybersecurity.

In Mexico, government groups have promoted proposals related to Internet control (regulation of content in social networks, regulation of content by ISPs, proposals to legalize espionage). Fortunately these have been countered thanks to local collaborations between organizations specialized in technical, legal and human rights issues. At the same time, #SeguridadDigital mentioned that the president's speech is greatly damaging the support that may exist for the work of journalists and activists in terms of freedom of expression.

In Brazil something similar occurs, although there is no specific legislation aimed at attacking human rights, but there is a great instrumentalization of the laws to criminalize social movements and civil society organizations.

Likewise, in Central American countries such as Guatemala, El Salvador, Honduras, Nicaragua and Costa Rica, legislations may vary, but common concerns include laws restricting freedom of expression online, unchecked mass surveillance, internet censorship and lack of protection of digital privacy.

For the time being, in Chile, control in the digital space is under construction, although organizations fear that public policies and laws that begin to address it will be generated. In fact, this same lack of legislation allowed many organizations and activists to have their communications tapped during the Revolt of 2019.

Also in Argentina, there are processes in place to implement biometric surveillance cameras, aiming to control society in general, in addition to surveillance processes through social networks exclusive to activists, as mentioned by 0xche.

Similarly, the laws on the dissemination of images without consent often allow the wording to be used for revictimization or to restrict other rights such as freedom of expression in

Mexico with the so-called Olimpia Law, which has thirty-two local and federal legislations throughout the country.

Vita Activa mentions that in this matter there are different legislations at a regional level, for example in Argentina (digital violence was recently included within the Law for the Comprehensive Protection of Women, referred to as 'Ley Olimpia Argentina'), in Brazil (same case as Argentina, it was included in the Law for the Protection of Women), in Bolivia (the Criminal Code), in Chile (normal related to online violence against children, and adolescents, and as far as adults, in the unauthorized dissemination of sexual content), in Ecuador (same case as in Argentina and Brazil), in Perú (the Criminal Code on harassment, sexual harassment, sexual bribes, dissemination of images, audiovisual materials or audios with sexual content, in Uruguay and Paraguay (also included within the Law for the Comprehensive Protection of Women).

Fundación Acceso makes mention of the importance of monitoring regulations and legal frameworks meant to challenge the digital rights of people and organizations, as well as knowing and promoting laws that protect basic rights online and promote digital security without compromising human rights.

Conclusions and recommendations

Throughout this work we have shared information concerning civil society organizations and collectives who are providing trainings, creating tools, *study plans*, and who conduct analysis to address digital security from different viewpoints.

- comprehensive security,
- a perspective of human, feminist and holistic rights,
- methodologies which ask for the participation and creation of joint knowledge: the popular pedagogies and popular feminist pedagogies.
- Although the challenges that were found have to do with two major areas:
- Time invested, given how urgent this is because of the clear risk involved in their practices, or rather because they have already suffered an attack, although it would be necessary to participate in a longer process, with methodologies adopted to both the context and the participants.
- The implementation of laws or use of legal mechanisms which harm and follow activists or communicators, the increase of online violence (especially towards women and individuals from the LGTBI+ community), the implementation of biometric surveillance, through spyware (such as Pegasus) or social media, particularly against activists, journalists or migrants.

In the midst of all this, civil society however has managed to gain the sufficient knowledge and achievements to be able to move on forward to ideas that are well worth sharing to better understand these processes:

• the trust people are creating in regard to technology, or technological appropriation.

• the *feedback* provided by participants as one of the greatest achievements for those organizations imparting workshops, create medium- or long-term accompaniment that does provide but does not establish the necessary confidence and reference.

• the effort to translate the technical into simpler words and, sometimes, even in fun ways, is recognized. While it is not easy to make people fall in love with digital security, it is crucial to make progress in the loss of fear and the reappropriation of the digital experience with confidence and security.

• Increased digital security awareness (sensitizations), knowledge of best practices around the subject and promoting the acquisition of technical skills and the ability to protect devices are essential for trainings.

• organizations are placing individual and collective care front and center. Little by little they have included approaches that leave aside simple technical matters to move on and begin the conversations on the importance of care as a prevention method.

• the importance of feminism in regional social movements, as well as its learnings are very valid as well for the digital realm, which at the end of the day is only another space in the actions of social collectivities.

• it is attempted to speak of security taking as a starting point the logic of care, as well as that of our life stories, believing that it is necessary to place both knowledge and group experience at the heart of things so that based on those experiences it is possible to create an identity with sufficient knowledge about digital care. They do not nurture fear nor bring up horror stories.

Finally, inhabiting the internet and socio-technical networks means exploring them, using them, changing them to adapt them to our needs, beyond the interests of those who created them.

In this research we also noted the openness of the organizations to support initiatives to think and analyze ourselves, as this one has attempted to do, with kindness and attention we have received they were all open to being interviewed, despite having full agendas with a multitude of activities. As well as all the materials and resources being offered within their websites to share and enrich each other, improve, update or analyze what we do and the contexts in which we do it.

Among the general recommendations we found throughout this research are the following:

- Create spaces for active listening with the individuals attending the workshops, to acknowledge the fact that not every share the same experiences, the latter may vary depending on age, territory and gender, among others.
- Receive feedback and ensure that communities take ownership of their own tools. Invest time on this second listening and strengthen these accompaniments.
- Promote the use of free technologies, which are easier to mold to specific needs.
- Dedicate time to update their knowledge, based on the need of understanding what is going on and provide solutions.
- Give way to transform digital security into digital care, within a more comprehensive process, that seeks the more collective and less individualistic connection of technologies.

The construction and socialization of this knowledge is necessary to prevent and monitor digital attacks. Therefore, we propose that a revised version of the global report be publicly disseminated in several languages, and if there is the possibility of creating lines of research to work in more depth on the various aspects covered here, such as training methodologies, analysis of training materials, limits and scope of digital security training, systematization of experiences, documentation of digital incidents in the region, among other topics to be developed with months of dedication.

It is important to continue building this research to truly understand what is the regional context on how digital security is being addressed, and to fully understand both the individuals and collectives that continue to work, as well as the tools we may use independently. Also, to share the results of different structures and organization networks that already exist, plus promote regional meets to exchange analysis and experiences.

APPENDIX 1

Organizations

Nombre	Sitio web	País / Región
Luchadoras	www.luchadoras.mx	México
SocialTIC	socialtic.org/	México
Sursiendo	sursiendo.com.mx	México
Tierra Común	tierracomun.org/	México
#SeguridadDigital	seguridad.digital/	México
María Lab	marialab.org/	Brasil
Red Transfeminista de Cuidados Digitales	dxche.org/	Brasil
OXhe	oxhe.org/	Argentina
Comuna Digital Laboratorio de conocimiento Libre	comunadigital.ec/	Ecuador
IPANDETEC	www.ipandetec.org/	Panamá
Centro de Autonomía Digital	autonomia.digital/	Ecuador
Fundación Karisma	web.karisma.org.co/	Colombia
Colnodo	colnodo.apc.org/	Colombia
Fundación Acceso	www.acceso.or.cr/	Centroamérica
Coding Rights	codingrights.org/	Brasil
InternetLab	internetlab.org.br/	Brasil
Nicaragua Cibersegura	www.linkedin.com/in/nicaragua-cibersegura-092a03181/	Nicaragua
Barracón Digital	barracondigital.org/	Honduras
ADC	adc.org.ar/	Argentina
RHyEH Hacklab	rhyeh.net/	Argentina
ElM Defensoras	elm-defensoras.org/	Guatemala
OpenLab	openlab.ec/	Ecuador
Hipertexto	hiperderecho.org/	Perú
La Libre Tecnologías comunitarias	lablibre.noblogs.org/	Ecuador
Internet Bolivia	internetbolivia.org/	Bolivia
Access Now	www.apc.org/	Regional
APC	www.apc.org/	Regional
Sulá Batsú	sulabatsu.com/	Costa Rica

Código Sur	codigosur.org/	Costa Rica
Tedic	www.tedic.org/	Paraguay
Derechos Digitales	www.derechosdigitales.org/	Chile
Colectivo Dissonancia	colectivodissonancia.cl/	Chile
Red en Defensa de los Derechos Digitales	r3d.mx/	México
Veta Activa	vita-activa.org/	México
ONG Amaranta	amaranta.org/	Chile
Ciberseguras	ciberseguras.org/	Regional
Cultivando Género	cultivandogenero.mx/	México
Colibres	colibres.org/	México
Técnicas Rudas	tecnicarudas.mx/	México

Redes - Alianzas

Nombre	Sitio web	País / Región
APC	www.apc.org/	Global
¡Dominemos la tecnología!	www.apc.org/	Global
Sul Sur	www.sul-sur.org/	Regional
Red Iberoamericana de Protección de Datos	redipd.org/	Regional
Alianza por el Cifrado en Latinoamérica y Caribe, AC-LAC	lac-ic.org/	Regional
Digital Defenders Partnership	www.digitaldefenders.org/	Regional
The Engine Room	www.theengineroom.org/	Global
ARTICLE 19 Programa de Derechos Digitales	articulo19.org/	México Centroamérica
Intervozes	intervozes.org.br/	Brasil
Tor	www.torproject.org/	Global
Observatorio Latinoamericano de Amenazas Digitales (OLAD)	latamthreats.digital/	Global
Internet Ciudadana	lac.internetciudadana.org/	Regional

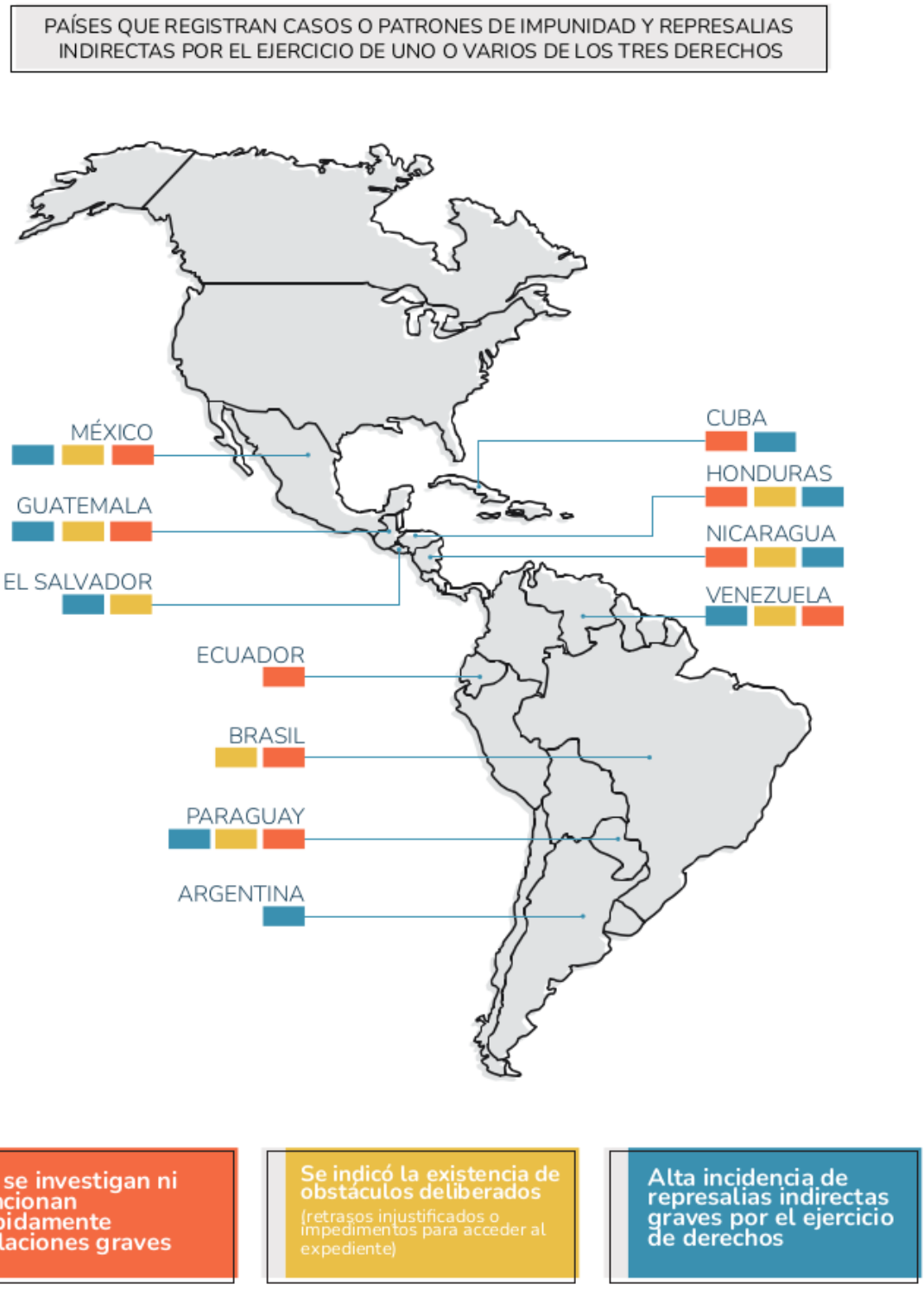
APPENDIX 2

Resources & materials

TITULO	Pais/Región	Tipo de recurso	Autoria	Temáticas
El caos de las contraseñas	Post de blog	TEDIC	seguridad digital, contraseñas	contraseñas, privacidad
El caos de las contraseñas preguntas frecuentes	Post de blog	TEDIC	seguras	
Respaldos, protegiendo lo más importante de tu organización	Post de blog	TEDIC	software libre, privacidad, seguridad digital	Guarani
Videos de Seguridad Digital en Idiomas	blog, video	TEDIC	seguridad digital, contraseñas	
Nos cuidamos online	web	TEDIC	seguridad digital, privacidad	
Cómo cuidar tu salud mental como periodista frente a la violencias de género en linea: Una gula	blog, video	TEDIC	seguridad, violencias de género en linea	
Toolkit de seguridad digital para marchas	fanzine	TEDIC	seguridad digital	
Manifestaciones libres: gula sobre la vigilancia policial en manifestaciones	Gula	TEDIC	investigación, privacidad	Jen Paraguay
Free the niple paraguay	blog, video	TEDIC	Investigación, privacidad.	moderación de contenidos
Libres y segures en internet	web	TEDIC	seguridad digital, salud mental, seguridad digital	
Mente en linea	web	TEDIC		
Fiesta antivurus: asi hackeamos el Jenicieno	blog, video	TEDIC	derechos digitales, género, tecnologia, violencia de género en linea	

Cyborgfeminista	web	TEDIC		
Consejos: Privacidad y seguridad digital en redes sociales	informe	Hiperderecho	Seguridad digital, redes sociales, privacidad	seguridad digital, privacidad, derechos humanos
¿Quién vigila a los vigilantes?	Web	Hperderecho	seguridad digital	
Kit de cibercuidados para activistas.	Gula	Hiperderecho	seguridad digital, modelo de riesgos	
Seguridad digital para cuidar nuestro activismo y reapropiamos de Internet		Hiperderecho	seguridad digital	
ACuerpándonos pruuna internet feminista, diversa y libre de autoformación: ¿Cómo podemos realizar nuestro taller ciberfeminista?	Gula	Hiperderecho	seguridad digital, ciberfeminismo	
Después de la ley	Web	Hperderecho	violencia de género en linea, asesoria legal	violencia de género en linea
Tecnaresistencias	web	Hiperderecho	Inea, asesoria legal	
Autocuidado y sororidad en linea para decidir. Gula para activistas en linea por la libre información sobre el aborto	Gula	Hiperderecho	autocuidado, tecnologia	
Conectad@s sin fronteras. La alfabetización digital como herramienta de crecimiento y autocuidado colectivo	Gula	Hiperderecho	migración, seguridad digital	
Blog Hiperderecho	Web	Hiperderecho	seguridad, privaciad, libertad de expresión	
Cuidados digitales y filantropia: Hallazgos y recomendaciones básicas	Gula	Maria Lab	cuidados digitales	
Guia de proteção para defensoras e defensores de direitos humanos	Gula	Maria Lab	cuidados digitales	
A Autonomia tecnológica como uma constelação de expertencias	Gula	Maria Lab	cuidados digitales	
Barricadas, estratégias e coletividade:	Gula	Maria Lab	cuidados digitales	

APPENDIX 3



Fuente: Libertades en retroceso, entre el Autoritarismo y la Defensa de la Democracia en América Latina, elaborado por la Asociación Civil Espacio Público para la Alianza Regional por la Libre Expresión e Información (2023)