Systematizing our digital security accompaniment from 2018–2020: findings and reflections

COLLECTIVE APPROPRIATION[1] = AWARENESS + PRAXIS + REFLECTION + DECISION MAKING

Systematizing our digital security accompaniment from 2018-2020: findings and reflections

1 Sursiendo defines technological appropriation as a process of acknowledging our digital needs and choosing what tools we want to use, develop capacities and make changes to become more familiar and comfortable with technology. When possible, we try to choose free/libre —free as in freedom— and reliable tech that allow us to inhabit our 'digital life' in a long journey towards technological autonomy and self-determination.

COLLECTIVE APPROPRIATION = AWARENESS + PRAXIS + REFLECTION + DECISION MAKING.

Systematizing our digital security accompaniment from 2018-2020: findings and reflections.

Chiapas, México. March 2021

Systematization Coordination: la_jes
Systematization design and development: Valentina Auletta
Texts and editing: Valentina Auletta, la_jes, dom
Design, layout and illustration: Diana Moreno
English translation: Nàdege

This research was conducted by Sursiendo with the financial support of Open Technolgy Fund and Digital Defenders Partnership.

In the night of these times of
surveillance and control
we want to learn how to learn from others,
situate ourselves in the world even despite darkness;
we look at the bats because they live together
and learn from each other
discovering new routes
new ways and meanings;
caring for others, receiving care
to fly through waves
towards shared knowledge
preserved as a contribution to humanity
connected to Nature
each bat offers it's pollination
and honors the planet that shelters us

Exquisite corpse, Sursiendo staff, March 2020

Tracing back our steps, pausing, observing each one to grasp that our journey doesn't fit in this society of progress, where "lo que pasó pasó..."[2] and we tend to bury the past.

But in Sursiendo, we firmly believe that you can't look ahead without knowing what you left behind; if not, you will keep on planting and harvesting the same things and the fruit will rot. It's necessary to observe the footsteps of those before us that have traveled the same path, or others alike that we haven't had time or the energy to explore.

In this spirit, in October 2019, Sursiendo **decided to embark a big challenge**: we wanted to review our process of "Digital Security Accompaniment for Grassroot Organizations in Chiapas 2018-2020" (DSA-2020) and extract meaningful lessons that allow us to understand and improve our work, as well as sharing this information with others.

2 "Lo que pasó, pasó..." refers to a popular reggaeton song and literally means "What happened, happened".

Even though DSA continues, we decided to frame our systematization until April 2020. In our workshops and within our organization, we also decided to inspire ourselves in non-human species. We took bats as a reference, animals that through ultrasound learn from each other, reading echoes (which are emissions from the past).

The DSA 2018-2020 initiative seeks **to mitigate digital risks** that grassroot human rights (particularly land, women, migrant, environment rights) movements face in their activism and work. The systematized process lasted 28 months, from January 2018 to April 2020 and began with an initial assessment.

Our work focused on San Cristóbal de Las Casas (Chiapas), though we also collaborated with people from other parts of the State like Tonalá, Palenque and Comitán. This region is particularly important because Chiapas is a State full of biodiversity and natural commons. It's native population is predominantly indigenous and because the State borders with Guatemala, it becomes part of the migrant route for Centroamericans. As a result, there are many human right defenders, as well as indigenous and rural communities in resistance against extractive industry that suffer violence, criminalization and prosecution, with a particularly high rate of violence against women and non binary people.

The support that Sursiendo provides has always intended to be **long-term and comprehensive**: from a critical political perspective on

technology, to digital security capacity building, personalized technical support, digital security incident documentation; and organizational protocol and policy design.

All these features make DSA 2018-2020 a new type of experience in digital security and has encouraged us to revive the process, unpack and re-elaborate this puzzle that reveals new parts.

This document is a summary of the **full systematization report** in which we intend to share our findings with those who want to or already are implementing digital security accompaniment. This is for our "future selves", for those organizations, collectives and allies that work in collective digital care. We hope that these lessons allow us to engage with what other people have learned and, through this exchange, embark in new collective experiences that contribute to transforming reality.

METHODOLOGICAL DESIGN

When we talk about systematizing experience, we refer to:

> *The process of going through an experience; recovering, organizing and analyzing information for further interpretation; transforming through sharing lived experience.*

(Sursiendo staff, October 2020)

Inspired by those who have theorized on Action-Research methodologies and ventured into systematizing their own experience, in Sursiendo we collectively designed our systematization framework; defining goals, questions and pivots to guide us throughout the process.

Research question	How did the Digital Security Accompaniment for grassroot human right movements in Chiapas, developed and implemented by Sursiendo from 2018 to 2020, improve digital security?
Systematization goal	The Digital Security Accompaniment (DSA) focused on 8 grassroot human right groups in Chiapas. It was designed, developed and implemented by Sursiendo from January 2018 to April 2020.
Goals	**Main goal** To understand how the DSA process has facilitated changes in the ways human right defenders become familiar and comfortable with digital security tools, and change habits and attitudes in consequence. This understanding will help us improve our future action. **Secondary goals** To share our experience regarding DSA, in particular self-assessment aspects, with other digital security and technology appropriation accompaniment initiatives. To influence civil society organizations and funders on the importance of implementing digital security long-term accompaniments.
Fundamental axis of meaning	**COMPREHENSIVENESS** We conceive comprehensiveness as a framework that seeks to facilitate appropriation from different perspectives: political, technical, physical, playful, economical and educational. We are interested in exploring the interplay of comprehensiveness and appropriation, framed as a change in attitudes, habits and acquiring tools within the accompanied organizations.

After the initial stage, we established a systematization route, "a method made up of five moments" (Jara, 2018) that helped us translate our lived experience into lessons.

- **Stage 0 - Experience:** accompaniment provided by Sursiendo to organizations in Chiapas.
- **Stage 1 - Methodological Design:** systematization road-map design.
- **Stage 2 - Historical Reconstruction:** based on document revision and 1:1 interviews with Sursiendo staff, we reconstructed the experience and identified important and relevant moments.
- **Stage 3 - Main characters' voices:** through interviews and surveys, we gathered a range of points of view from the different organizations involved.
- **Stage 4 - Critical Interpretation:** within the Sursiendo accompaniment team, guided by a series of learning goals.

Our guiding principles are:

- **A "dialogue of knowledge".** a principle of Popular Education that guides participatory Action research by which "no-one thinks in someone else's head; each one of us has something to contribute to the collective pool of knowledge" (Jes, 9th of October 2019). This perspective dissolves the academic research dichotomy 'subject-object' and disciplinary boundaries.

- **"Walking and asking".** From the myth "Ik'al and Votán" narrated by Don Antonio. "And that's how the true women and men learned that questions help us walk and not just stay still. Since then, the true women and men ask questions to continue their path. When they arrive, they say goodbye; and when they leave, they say hello. They are never still" (EZLN - Zapatista Army of National Liberation. 13th December of 1994).

- **"Self-study" and "collaboration"**, key components of the libre free software philosophy.

- **"To learn how to learn"**, step by step learning process that encourages autonomy.

- **Against extractivism! including epistemic extractivism** (Grosfoguel, 2016). Knowledge is a commons that can be developed and looked after in collective.

The process took into account a wide range of research methods, prioritizing those that allow free expression and in-depth reflective dialogue. In the collective Digital Security Accompaniment workshops implemented, we used techniques such as "brainstorming", "exquisite corpse" and "timelines" that helped us think together and draw conclusions through individual reflection and collective debate based on guiding questions. We also performed semi-structured interviews with the Digital Security Accompaniment team, as well as representatives and focal points of the accompanied organizations. Additionally, we handed out surveys to all participants.

We picture our advances **as a spiral**; in other words, we give time and space to go back and review each phase with a more granular interpretation and understanding.

Among the aspects we celebrate in this process, we acknowledge the methodology we followed: it is participatory, inspired in Popular Education and uses non-digital tools to encourage collective thinking. We were able to facilitate an open conversation between the experience, what was happening, and the people involved.

We also celebrate the opportunity we had to **develop meaningful lessons** for future accompaniment (by us or others) and for our organization. We were also able to render guidelines to take into account for future systematization.

Like any other experience, we also encountered certain challenges. Some were external, like Covid-19 and the health emergency it implies; and others were internal, particularly related to insufficient and/or disorganized documentation and interpersonal conflict within Sursiendo.

Throughout the systematization process, we also stumbled upon mistakes and we are aware of some limits regarding the experience we set out to systematize: a short —barely two years— process, centered in Chiapas and led by only one organization: Sursiendo. The Digital Security Accompaniment 2018-2019 was Sursiendo's first attempt in performing simultaneously long-term accompaniment with several organizations, as well as conducting a final systematization.

On the other side, the fact that different people led different stages of the process (assessment and implementation), long with staff turnover limited, to a certain extent, the learning potential of this systematization.

Perhaps the findings here described can't be generalized because they are very specific to the groups we have accompanied: organizations from Chiapas that, through their interest in holistic security, committed to a digital security accompaniment.

Among the mistakes encountered, we point out not having included in the systematization the perspectives of the organizations that didn't finish the accompaniment process. Regarding the research techniques implemented, we consider that the individual interviews conducted to the DSA team didn't provide sufficient information in comparison to the collective workshops where we were able to unpack, reconstruct, analyze and interpret the experience based on each person's subjective input.

All over, systematizing the Sursiendo Digital Security Accompaniment 2018-2019 was a positive and innovative initiative in the digital security field that **will open up opportunities** for us to engage with other experiences in Latin America.

FINDINGS

Systematizing the Digital Security Accompaniment initiative implied encountering findings in each step of the process. Each document we reviewed, each discussion we had, each story shared by participants allowed us to understand better the more visible and deep aspects of each event, connect the dots between moment and moment, extrapolate factors that facilitated each context and articulate lessons to hold on to.

Firstly, we understood the main underlying motivations of the organizations that completed the accompaniment process and identified in them the determination to invest in their own institutional digital security. Despite the particularities of each organization, the general interest towards Digital Security was the awareness of it's impact on different layers of institutional risk.

Throughout the process, we observed that all participant organizations had experienced some type of digital security incident between 2014 and 2018 related to the national and international context. We highlight as particularly relevant incidents like Snowden's global surveillance revelations and #GobiernoEspía (#GovernmentSurveillance) which exposed Mexican Governmental —at the time, under Peña Nieto presidency— use of spy surveillance software.

> *We observed this in a comprehensive way. Our concern was around security; security at a physical, digital and emotional level. We have tried to give attention to this in the past without success but now, due to the context, it becomes relevant and urgent. We have decided to make a move.*
>
> **(Focal contact, Women rights organization, April 2020)**

Another organization points out institutional funder pressure as an external factor to invest in digital security:

> *One contextual factor are funders, at least the ones we are working with. They started to ask us about our digital security measures, how we are looking after ourselves, our communication channels and that made us think that it's going to be more and more necessary to understand our needs in these aspects.*
>
> **(Director, Migration rights organization, April 2020)**

Among the most significant changes stemming from the accompaniment, we highlight an increase in awareness regarding digital threats and risks:

> *We've gone from experiencing direct attacks to mass media and cyber attacks. The learning process with Sursiendo has really helped us see this new element and become more alert in this sense. It's much more easy to undermine, attack or call out online than face-to-face. Through many conversations with Sursiendo, we realized that we were oblivious to all of this. Our analysis was completely transformed. We didn't imagine these things were attacks. And now we look back, we understand that the attacks and blows were coming from this side.*
>
> **(Director, Human rights organization, April 2020)**

Additionally, we point out a shift in attitudes related to cellphones and creating digital security protocols.

An aspect that both organization directors and members, as well as the Digital Security Accompaniment team appreciated was the fact we implemented group sessions dedicated to building organizational digital security improvement proposals, in other words, we created digital security mechanisms and procedures for each organization where we addressed specific issues:

> *We had many conversations within the organization and with Sursiendo that gave us the opportunity to examine our flaws and trace new directions.*
>
> **(Director, Human rights organization, April 2020)**

This shows us that drawing from reality is an appropriate methodological approach to understanding digital security in a meaningful way: to analyze the situation we are in, map incidents and develop, step by step, personalized measures. That's what being comprehensive is about.

All the organizations involved agree that the most tedious part of the accompaniment was the theory, sometimes explained through complex language, in particular the discussions on libre free software. Other aspects to be improved include the amount of content (we covered too much) and the frequency of the workshops that resulted in

organizations loosing focus on the accompaniment, specially groups with a lot of members.

Most of the accompanied organizations perceive our **work methodology** as successful and, for some, even innovative. They particularly appreciated our availability, knowledge, skills, the dynamics and exercises we implemented in small group sessions, the hardware tech support we provided, our commitment to free libre software; along with offering them the opportunity to...

> *...find out about the story of things.*
>
> **(Director, Migration rights organization, April 2020)**

> *I vividly recall the first workshop session and thinking "Awesome, they're working with participatory creative methodology". Because, sometimes, when you address topics that participants may consider more technical, it becomes boring. I specially remember the traffic light exercise for identifying risks. I even thought "when can I use this again", not necessarily in the same way, but for other types of risk analysis. I think that really engaged us because it "wasn't just talking about tools but about political issues, actual risks that grow day by day.*
>
> **(Director, Human rights observation organization)**

Despite the challenges involved, we all appreciated the experience of collective learning. One of the organization directors highlights the importance of collective decision making in this type of process:

> If it has an impact on our security and involves the whole team, the agreement needs to be discussed among all of us and not made unilaterally.

(Director, Human rights organization, April 2020)

After listening to the key people involved in the DSA 2018-2020, Sursiendo staff focused on interpreting the results which allowed us to identify the main enabling factors (those that help develop the accompaniment and achieve results) and impeding factors (those that hinder the accompaniment and it's results), essential to improve how we design our work in the future.

In Sursiendo, when we started designing the accompaniment and selecting the organizations, we already had an **appropriate contextual understanding** of human rights defense in Chiapas and the ecosystem of organizations. In the past, we had already collaborated with some of them, which gave us experience to base our work on.

Having an **innovative approach** in the local context of our work, based on participatory popular education methodology and our experience with different regional grassroot movements, had a positive impact on the activities we implemented; designed long-term according to the specific needs of each accompanied organization, putting into practice a personalized comprehensive approach. In our initial assessment, we discovered that one of the complex factors in the process of acquiring digital security tools is the lack of reliable technical support and a long-term process that takes into account the needs and pace of the people involved. From our perspective as Sursiendo, we understand that human right organizations in Chiapas are not so familiar with technology issues. We wanted to make them more comprehensive and accessible through activities that demystify tech as something only for experts and, instead, present technology as something we can learn. Generally speaking, participants were committed, understood how their organization operated and were part of the internal decision making process.

In addition, the **focal points** of the accompaniment showed interest and were familiar with technology. All of these factors encouraged the accompanied groups in claiming the workshop contents and adapting them to their contexts, making this whole process more sustainable.

Regarding **impeding factors**, we identify deficiencies in our intervention design, in particular in the definition of goals, expected results,

indicators and monitoring. We didn't include raising awareness as part of our result framework despite it being essential in collective appropriation.

From the beginning, there was an **ambiguity regarding the limits and scope of the tech support we could provide**, resulting in different expectations within the accompanied organizations. Some of them assumed that Sursiendo would give general tech support, beyond issues related to the digital security accompaniment. Processing these petitions became problematic at times.

Likewise, **the workshop agenda had too much content**, even after revision and synthesis, and this made it more difficult, particularly in larger groups, for people to assimilate all the information. Now we know this is a result of a lack of following up on the different organizational needs we identified during the initial assessment.

Lastly, we are aware that the Digital Security Accompaniment initiative is our first (comprehensive) long-term accompaniment process as Sursiendo and this fact can be considered the main reason of the challenges and drawbacks that came up.

We observe a lack of references and experiences regarding long-term digital security accompaniment for human right defenders. This is still in process.

Interpretation helped us articulate a series of **general lessons**, in particular related to collective appropriation.

Human right defenders in Latin America are becoming more and more aware of their own digital security needs, most of the times because they have experienced situations that have put them and their work at risk.

We note that **collective technological appropriation** is a slow process, achieved step by step: individual awareness of the surveillance context and the risks related to technology that affect human right defenders; individual hands-on practice with tools that improve security; collective analysis and discussion of the incidents and threats encountered when working in human rights; collective decision making that translates into designing security strategies and protocols.

COLLECTIVE APPROPRIATION = AWARENESS + PRAXIS + REFLECTION + DECISION MAKING

Lastly, we highlight the importance of decentralizing digital security and tech capacity building consultancy and mentoring into a more local model. Organizations such as Sursiendo, both involved at a local and connected with global level, seek to **create connections** for the groups they support.

At present, most organizations have technical needs but don't always have access to trustworthy tech support, among other reasons, due to a huge technological gap. Unreliable tech support, specially in "high risk" contexts, can expose organizations (to risks, to fear and paranoia) more than help them. For this reason, it's essential to provide sustainable tech support as part of digital security accompaniment.

Organizations need their own resources to cover tech support. When doing digital security accompaniment, we must make emphasis in the relevance of assigning specific resources to this aspect and pass this message to funders.

OUTCOMES

To wrap up, we would like to offer some basic tips for those who face the challenging but satisfying task of planning and implementing digital security accompaniment for human right defenders.

How to start?

You have to be familiar with the human right defense context where you are going to work so you can center accompaniment in local needs.

Designing the process is a very important aspect that requires time, resources and, ideally, the participation of the whole accompaniment team.

We believe that developing consistent digital security accompaniment strategies in each stage of the process is essential: from the design, staff induction, planning, implementation, follow-up to monitoring and assessment phase; threading a *continuum* between the assessment and workshop, tech support and follow-up steps of the process.

We advise performing a comprehensive assessment at the beginning of the accompaniment including contextual elements and aspects that help understand in depth the organizations involved (internal dynamics, technological aspects, characteristics). You will establish the expected goals and results based on these aspects and, inevitably, they will be different for each organization.

Two particularly important elements when selecting organizations that will receive accompaniment are :

The amount of digital risk the organization faces. This factor tends to determine the interest the organization shows and sustains regarding digital security. Organizations that face more digital risk, that have experienced serious digital security incidents, are more aware of the risk and, in consequence, consider digital security as an institutional priority, facilitating tremendously accompaniment.

The degree of articulation and internal cohesion within the organization. Some organizations have a lot of staff turnover or have certain areas that aren't so articulate; meanwhile others have clear internal structures and decision making procedures which make accompaniment easier.

We also recommend that the decision and intention to embark on an accompaniment comes from the actual organization, in order to share the responsibility of the process. We discourage working with unknown organizations unless there is some kind of reference from third parties and contacts.

What do we need to move forward?

Digital security accompaniment can be designed and implemented in many ways depending on the features and needs of each context and everyone involved. A personalized approach can translate into different teaching and learning routes to acquire skills and/or tools.

Yet, there are some general aspects that are worth paying particular attention to. Like in any accompaniment process, it's important to

choose the people that will be in charge of the implementation. Even though there are some detailed specifics, **digital security is nested in holistic security.** You don't have to be an expert in the field, but, working with organizations during a long time span and having enough awareness regarding holistic security is essential in digital security accompaniment.

In order to commit to a holistic approach, digital security accompaniment trainers should consider on-going holistic security capacity building.

Looking after the relationship, spending time and using specific methodology to bond with the accompanied organizations is fundamental. This nurtures trust that, on a long-term, helps address conflicts that can come up in the accompaniment.

In this sense, we recommend establishing and writing down shared agreements to check you are all on the same page. You should consider a range of aspects regarding the process and attempt to clarify what is being offered and what to do in case of an emergency.

In digital security accompaniment, **choosing a focal point** within each accompanied organization is important. Ideally, this person is familiarized or has a particular interest in technology and also has a leading role within the organization. They will be in charge of the activity organization logistics, of day-to-day tasks and bridge between the organization and the trainers.

In addition, if the accompanied organization has a vertical structure, you will need to maintain communication with the leads, address decision making and follow up, making sure to keep an open on-going flow of information between all parties (trainers, organization, leads).

Digital security accompaniment provides space to reflect within the core accompaniment team and assess what is being done (using monitoring tools), exchanging subjective points of view in order to make any desired changes in the process.

How to assess a Digital Security Accompaniment?

Assessment and monitoring are essential aspects when measuring the scope and limits of an intervention, both during the process and at the end. They help determine how to follow up **and plan future interventions.** In this sense, we consider important to distinguish two dimensions: on one hand, the actual accompaniment assessment that must respond to the established design criteria and, on the other, internally, among the staff and project coordination.

For the later, having detailed profiles when implementing the accompaniment and pre-established activity assessment procedures will help follow up with the people that are implementing the accompaniment with the grassroot organizations and collectives. It will also help us identify the individual performance aspects that we need

to strengthen, both at a methodological level and educational level for workshops and training (technical, legal and holistic security). Finally, it will help us re-design better our activity implementation, both in our accompaniments and within our organization. It will also facilitate sharing our experience with other groups and people that are involved in similar digital security accompaniment initiatives.

Regarding **internal monitoring and assessment**, we consider important to establish specific moments for internal assessment, individually and collectively, in order to analyze merits and lessons throughout the process. For us, it's fundamental to maintain an approach centered in self-assessment and self-criticism along with feedback from peers. We also value encouraging an atmosphere of mutual trust based on assertive and non-violent communication.

As for **external monitoring and assessment**, we highlight the relevance of analysis tools that go beyond personal impressions and are based on collective exercises implemented in real-life contexts.

Apart from lots of learning, this systematization experience has left us with open questions. Firstly, we ask ourselves what tools can be more appropriate for assessing accompaniment. What other tools out there can we use? Should they be designed at the beginning of the process and remain the same until the end? Or should we review and adapt them throughout the process? If so, how often?

On the other hand, we are aware that, in order to provide a good accompaniment, it's important to understand the internal organizational structure of the groups you are going to work with: the ways they operate and learn, their structure and how they make decisions. How do we do this if we don't know the organizations beforehand? Observing how both sides (who accompanies and who is accompanied) walk together allows us to understand if the identified structures and types fit with how the organization works and acts in practice.

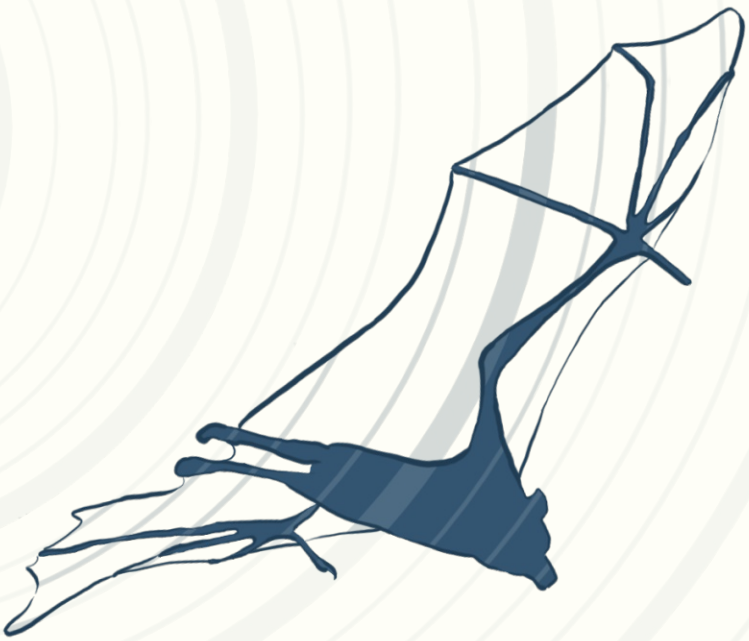
Lastly, what steps should we follow to accompany collectives that don't have a solid institutional structure? There are many challenges in this type of support, specially if their activism isn't paid for and they do it in their spare time, without a specific office or venue or schedule. Besides, activist collectives from the city and grassroot movements in rural areas are very different in how they engage and organize. How can we **address these particularities** in long term support?

We would love to talk about these issues with other groups that do similar work.

On a final note, we would like to repeat that the thoughts described above result from our specific experience: the experience of a small organization based in Chiapas that seeks to foster collective digital care among local human rights organizations. We focus on taking small steps, moving forward in spirals, while we trace back our path with firmer steps.

Even though, throughout this process, we have wanted to share our learning with other groups and people, we don't intend to "copy paste" or anyone else to do so, but **contribute to collective knowledge** with inspiration, tips and ideas to build a resistant digital culture.

Full of lessons, we are ready to embark new journeys, aware that what is certain today may not be tomorrow.



REFERENCES

Zapatista Army of National Liberation | EZLN (13th of December 1994). La historia de las preguntas. Chiapas. Disponible en: https://enlacezapatista.ezln.org.mx/1994/12/13/la-historia-de-las-preguntas/

Grosfoguel, R. (2016) Del extractivismo económico al extractivismo epistémico y ontológico. Revista Internacional de Comunicación y Desarrollo (RICD), 1(4), 33-45. Universidade de Santiago de Compostela.

Jara, O. (1994) Para sistematizar experiencias: una propuesta teórica y práctica. San José: Centro de Estudios y Publicaciones Alforja; Instituto Mexicano para el Desarrollo Comunitario.

Jara, O. (2018) La sistematización de experiencias: práctica y teoría para otros mundos posibles. Bogotá: Centro Internacional de Educación y Desarrollo Humano.

This report was made and designed with free software: Libre Office, Scribus, Inkscape and Krita. The following free fonts were used: The Bold Font for the titles, HK Grotesk for subtitles and for the body of the text.

Chiapas, México
March 2021