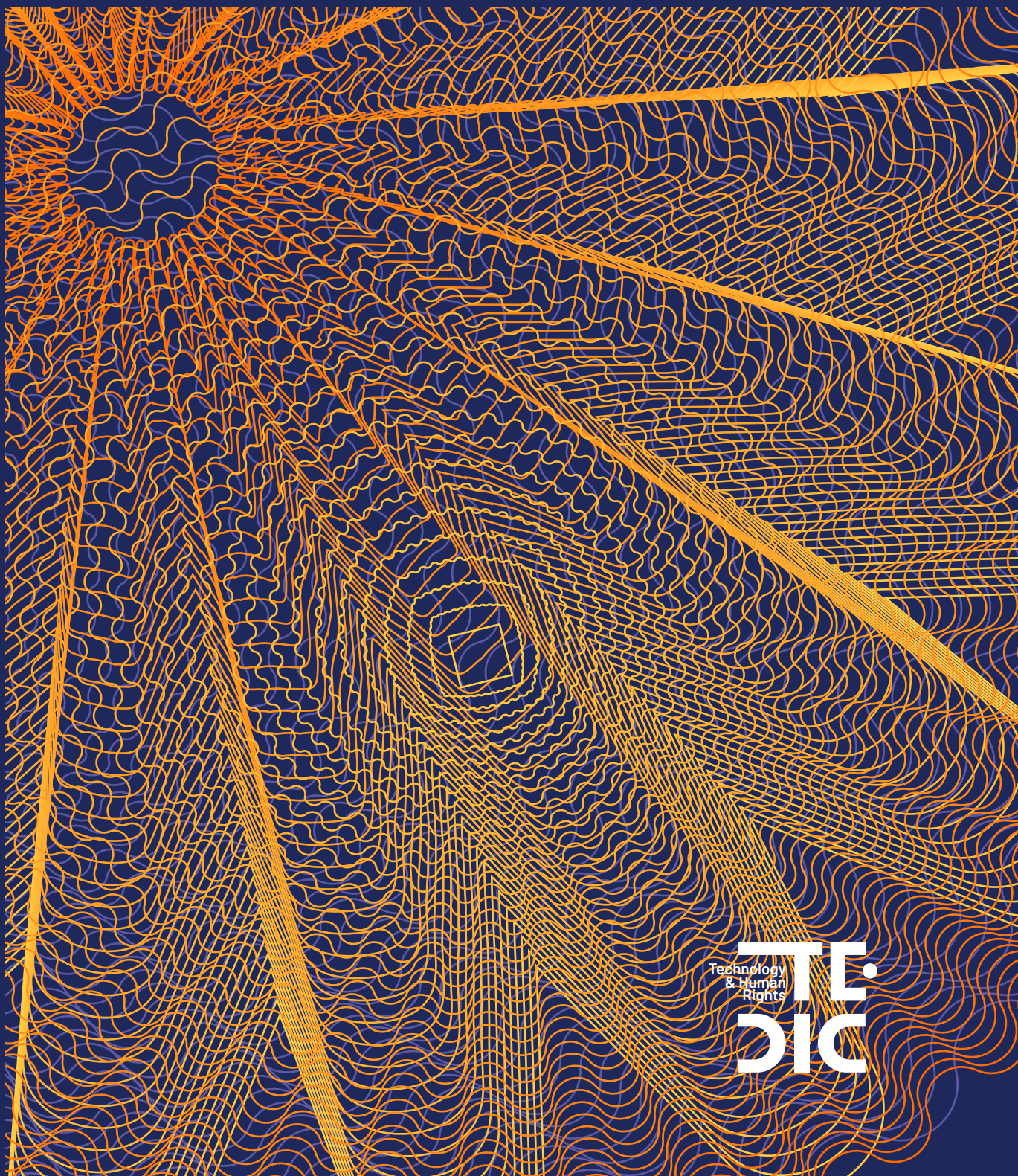
CYBERSECURITY FOR HUMAN RIGHTS DEFENDERS IN PARAGUAY



CYBERSECURITY FOR HUMAN RIGHTS DEFENDERS IN PARAGUAY

Technology & Human Rights

Digital Defenders Partnership is an international program aimed at strengthening the resilience of human rights defenders and organizations by improving their digital security through a holistic and sustainable approach.

This research was possible through support from the DDP Regional Partnership Fund, which supports initiatives that promote online freedom and digital protection for human rights defenders operating in a single country or region.

TEDIC is a Non-Governmental Organization founded in 2012, whose mission is the defense and promotion of human rights in the digital environment. Among its main issues of interest are freedom of expression, privacy, access to knowledge and gender on the Internet.

CICYBERSECURITY FOR HUMAN RIGHTS DEFENDERS IN PARAGUAY

SEPTEMBER 2024

RESEARCH
Mariela Cuevas

COORDINATION
Leonardo Gómez Berniga

METHODOLOGICAL DESIGN
Fundación Karisma - Colombia

MAPPING OF HUMAN RIGHTS DEFENDERS
Coordinadora de Derechos Humanos del Paraguay (CODEHUPY)

EDITING AND PROOFREADING
Maricarmen Sequera

LAYOUT
Horacio Oteiza

COMMUNICATION
Araceli Ramírez

INDEX

GLOSSARY

CERT-PY	Paraguay's Cyber Incident Response Center.
CICTE	Inter-American Committee Against Terrorism.
CISA	Cybersecurity and Infrastructure Security Agency.
CSIRT	Computer Security Incident Response Team.
CODEHUPY	Human Rights Coordinator of Paraguay.
HR	Human Rights.
DGCPI	Directorate General of Cybersecurity and Information Protection.
DDOS	Distributed Denial-of-Service, DDoS
ENC PY	National Cybersecurity Strategy of Paraguay.
EPH	Permanent Household Survey.
FGE	General Prosecutor's Office.
LGTBIQ+	Lesbian, Gay, Trans, Bisexual, Intersex and Queer. The plus sign refers to inclusion of all gender identities and sexual orientations.
MITIC	Ministry of Information and Communication Technologies.
MITM	Man-in-the-Middle.
OAS	Organization of American States.
OEE	State Agencies and Entities.
UN	United Nations.
SENATICS	National Secretariat of Information and Communication Technologies.
SICOM	Information and Communication Secretariat.
SQL	Structured Query Language.
ICT	Technology, Information and Communication.
XSS	Cross-site scripting.

RESEARCH SUMMARY

The research analyzes the cybersecurity situation of human rights defenders in Paraguay, focusing on understanding the dynamics of using the digital tool, Internet and its cybersecurity.

The defenders seek the protection and promotion of human rights from different dimensions and are key subjects to combat situations of injustice and arbitrariness in different issues, so they also strengthen the democratic quality and the safeguarding of rights. In view of the role they play in general, they are in a situation of risk and vulnerability in terms of security and, in particular, in terms of cybersecurity exposure.

In response to this situation, this research was conducted by TEDIC in Paraguay in collaboration with Fundación Karisma from Colombia. The aim was to gather information on the current state, risks, weaknesses, threats, and strengths of digital security, and to guide decision-making on protective measures for human rights organizations and defenders.

The research used a quantitative-qualitative methodology, and therefore made use of: -a mapping of human rights defenders and the application of a survey on digital security to 130 human rights defenders in Paraguay, the development of focus groups and in-depth interviews that made it possible to know more clearly the perceptions and knowledge in general about cybersecurity.

KEYWORDS: *cybersecurity, vulnerability, threats, cyberattack, digital violence, human rights defenders, human rights.*

METHODOLOGY

This research conducts an exploratory study to establish a baseline for data related to the cybersecurity of human rights defenders in Paraguay.

The work is based on the study "Strengthening the guarantee of the rights of human rights defenders, leaders, their organizations and collectives in Colombia" developed by the Karisma Foundation during the year 2023-2024 respectively.

Methodologically, both quantitative and qualitative research techniques were employed. For the quantitative approach, 130 surveys were applied to human rights defenders in Paraguay, completed both synchronously and asynchronously. The mapping of human rights defenders was provided by the Human Rights Coordinator of Paraguay (CODEHUPY). The selection considered the various geographical locations of the individuals across different parts of the country.

Asynchronous surveys were distributed to selected individuals in the human rights network via WhatsApp messaging, while synchronous surveys were conducted with assistance via telephone. Additionally, two focus groups were held with key figures in various human rights issues, and three in-depth interviews were conducted with key informants known for their expertise and knowledge in the fields of cybersecurity and/or human rights.

DATA COLLECTION TOOLS

the following details the mechanisms considered for each type of data collection tool:

Survey

The type of survey applied was descriptive in nature, collecting information from one hundred and thirty (130) human rights defenders in Paraguay. The asynchronous surveys were applied to one hundred and fifteen (115) profiles and the synchronous surveys to fifteen (15) profiles. The composition of the profiles surveyed was as follows: peasant defenders, indigenous defenders, defenders of the right to the city, environmental defenders, defenders of freedom of speech, defenders of the right to identity: feminists and LGTBIQ+, education defenders, health defenders and defenders of the rights of children and adolescents. The survey questionnaire was available through the Google forms tool.

Focus groups

Two (2) focus groups were conducted with the participation of 8 (eight) people per group. The participants included defenders from organizations working on various human rights issues (right to the city, peasants, LGTBIQ+, education, environment, among others). The instrument used to collect information was based on the categories and questions organized by the Karisma Foundation.

Interviews

Three (3) in-depth interviews were conducted with key informants recognized for their experience in the fields of cybersecurity and/or human rights. Individuals were selected based on the following profile: at least five (5) years of work in the field of human rights; a recognized track record in defending rights; individuals affiliated with human rights platforms, monitoring teams of cooperation entities, and/or civil society actors. The instrument used to collect information was based on the categories and questions organized by Fundación Karisma.

Review of secondary sources

To gather information from secondary sources, research related to cybersecurity and human rights was consulted, as well as public documentation related to the topic available in online repositories and those related to the United Nations Rapporteurships on Human Rights and Cybersecurity.

THEORETICAL FRAMEWORK

CONTEXT OF INTERNET USE

the daily use of technology by a large part of the population and the fact that people are connected to devices and the Internet is a characteristic of this time and has been a worldwide phenomenon since the end of the 20th century. In Paraguay, according to the Permanent Household Survey (EPH, 2023), the Paraguayan population using Internet is 76.3%, which represents approximately 4,556,000 people. The percentage growth from 2015 to 2022 has been 26.6% (From 49.7% to 76.3%).

The impact of Internet on people's lives is of unprecedented magnitude, as it has created a new space for interaction and connection known as cyberspace, where distances are shortened and borders are blurred. Today, accessing information is characterized by ease and speed.

The digital space is complex and continuously evolving. Discussing it involves recognizing certain factors that, according to Machín and Gazapo (2016), include the following elements:

1. Data
2. Computing technologies (Hardware, Software, Computer networks/Infrastructure, Network protocols, virtualization, cloud computing).
3. Analysis / Understanding Information Technologies
4. Interaction/Management Technologies (Human-Machine Interaction, Intelligent Agent Technologies, Personalization Technologies, Database Technologies)

The aforementioned authors indicate that the attack facilitated by technology can occur when an action is taken against one or more elements that make up cyberspace, thus perpetrating an operation with the aim of gaining access to and manipulating certain information.

The connection between cyberspace and security leads to the consideration of security from a harmonic perspective, as a public good, and from a conflict perspective, as a space of war. Acuña (2017) points out that "without a people-centered approach, cybersecurity only serves to give more power to power". Sancho (2017) indicates that the treatment of the Internet as a public good, obliges the State to develop actions to ensure minimum security conditions and thus enable the entire population to use it reliably.

WHAT IS CYBERSECURITY?

although cybersecurity is a term that has not achieved consensus on its definition, it can be said that it is an economic and social challenge, since it is not limited only to the technical dimension. In this sense, it refers to a set of measures and practices that seek to minimize risks related to digital security, and through this, contribute to socio-economic development, ensuring the protection of human rights and democratic values (OECD, 2016) [1].

It is important to contextualize security from a human rights perspective, as it frames security within the capacity of individuals to act freely and responsibly. Internet security policy should not be reduced to a defensive profile but should act as a facilitator in the protection and safeguarding of individuals' rights. Thus, it offers a positive perspective with solutions and a reduction of the negative view from threats (TEDIC, 2016).

Cybersecurity consists of ensuring the protection of people or organizations in cyberspace, specifically, it is about taking care of personal or institutional data to keep them away from threats on the Internet or the network. It involves addressing the human-machine relationship. Cybersecurity protection measures are aimed at safeguarding confidentiality, information (availability and authenticity) and data integrity of individuals, organizations, companies and the State. The need to incorporate the human rights approach becomes essential, particularly the rights to privacy, intimacy, confidentiality, availability and integrity of information, and freedom of expression (Karisma Foundation, 2024). In coincidence with the above, the publication of experts on Cybersecurity (Sequera et al, 2018), indicate that digital security is closely related to people, since the way in which policies regulating online behavior and information security are implemented, are closely related mainly to fundamental rights such as the right to privacy, freedom of expression or free association (p. 5). This reinforces the need to understand the definition of cybersecurity in view of the interdependent relationship between digital security and human rights, and in this way, therefore, give way to the effective safeguard of the security of people in the online and offline field.

Cybersecurity is compromised, vulnerable and threatened when perpetrators, attackers or malicious individuals carry out acts to gain unauthorized access to accounts, computer equipment or systems to commit some kind of attack for different purposes, such as information theft, fraud, extortion, harassment, spamming, among others.

It is important to point out that cybersecurity can also be attacked by State surveillance. Some of the ways in which digital security is violated are through mechanisms that can be used by the national police, such as: extraction of data from mobile phones (physically), hacking of mobile devices, extraction of data from the cloud, the use of facial and body recognition cameras in public spaces, and monitoring of social media of activists, among others (Sequera, 2022).

1 OECD (2016). Broadband policies for Latin America and the Caribbean: A handbook for the digital economy. Available at: https://read.oecd-ilibrary.org/science-and-technology/politicas-de-banda-ancha-para-america-latina-y-el-caribe/gestion-de-riesgos-de-seguridad-digital_9789264259027-17-es#page3. Accessed July 15, 2024.

The application of some examples mentioned above compromises certain rights that the National Constitution of Paraguay itself mentions in Article 33, such as the right to privacy, the right to inviolability of documentary heritage and communication, undermining the protection of personal data. State surveillance is one of the concerns and factors to be addressed when talking about cybersecurity. In the modern environment, telecommunications surveillance involves monitoring, intercepting, collecting, analyzing, using, preserving, storing, interfering with or obtaining information that includes or reflects a person's past, present or future communications, is derived or arises from them[2] (Sequera et al., 2016).

Surveillance in telecommunications from the use of biometric technology is one of the ways in which the national police implements control and undermines democracy by not guaranteeing the use of anonymity of people for their participation in debates or demonstrations of public interest (Carrillo et al., 2018). Currently, in Paraguay, by not having a comprehensive law on personal data, exposure and vulnerability in terms of digital security is exacerbated.

The authorship of the perpetrators corresponds to different typologies, such as, for example: attacks sponsored by the State or by other States, by the private sector, by terrorism or extremist groups, organized crime, low-profile attacks and attacks by staff members with privileged access (Sequera et al., 2023). It should be noted that online gender-based violence is one of the most frequent attacks on digital security in the country (Carrillo et al., 2024).

The impact of these attacks is classified in a low, medium or high range according to the magnitude of the incident (Sancho, 2017). In general, the literature points out that technology-facilitated attacks target governments and the private sector, but it also occurs with activist organizations of social causes, human rights defenders and individuals in general. These last two groups are also victims of attacks, whether through espionage, attacks on infrastructure, theft and publication of sensitive information, attacks on social media, among others. That is why this research addresses the issue of cybersecurity and human rights defenders to understand the current state of this sector in relation to their digital security.

It is important to consider fundamental aspects of cybersecurity when addressing the issue from public policies on digital security, thus, considering transparency and the inclusion of civil society, having a people-centered approach, recognizing their duties and protecting their rights, keeping constantly updated by the characteristics and dynamics of the phenomenon, are key aspects to enable social and economic development while ensuring human rights[3].

2 The authors Sequera, M. and Rolón Luna, J. (2016), use this definition based on the International Principles on the Application of Human Rights to Communications Surveillance (2014). https://es.necessaryandproportionate.org/text. Accessed on 05 July 2024.

3 These points mentioned are the result of the analysis and debate that took place in Colombia regarding cybersecurity, based on the draft of a Decree issued by the MinTIC. These criteria on digital security are also those recommended by the OECD (2016). Karisma Foundation (2024). Comments to the draft cybersecurity decree of the MinTIC. https://web.karisma.org.co/comentarios-al-borrador-del-decreto-de-ciberseguridad-del-mintic/. Accessed on 25 July 2024.

HUMAN RIGHTS DEFENDERS AND CYBERSECURITY

in 1998, the United Nations General Assembly[4] approved the Declaration on Human Rights Defenders, which deals with the right and duty of individuals, groups and institutions to promote and protect universally recognized human rights and fundamental freedoms. Specifically, the defenders seek the protection and promotion of human rights from different dimensions such as: development, fight against poverty, humanitarian and peace actions, civil, political, economic, social, cultural, environmental and digital rights, among others.

It is important to remember that many UN bodies have addressed this issue. In 2022, for example, the United Nations High Commissioner for Human Rights submitted a report to the Human Rights Council, expressing serious concerns about attacks on privacy by States. The Special Rapporteur on the right to freedom of peaceful assembly and association, Clément Voule, emphasized that we are facing a worrying increase in legislation and public policies aimed at combating cybercrime, which also opened the door to sanctioning and monitoring activists and protesters in many countries around the world[5].

In Paraguay, human rights defenders are key players in guaranteeing the promotion and protection of fundamental rights and, therefore, in combating situations of injustice and arbitrariness in different areas. As they play key roles in guaranteeing the quality of democracy and the safeguarding of rights, in general, they are in a situation of risk and vulnerability in terms of their security and protection and, in particular, in terms of cybersecurity exposure. In this regard, the proposed bill presented to the Paraguayan Congress is illustrative, as it addresses the need for the "Law for the Protection of Journalists, Communicators, and Human Rights Defenders".[6]

As mentioned above, the use and dependence on technology for the development of daily life have shown exponential growth in recent decades. Human rights defenders are not exempt from this phenomenon, and their advocacy work often involves the frequent use of digital platforms and communication channels, whether for coordinating, organizing, disseminating, or exchanging information. Specific or mass surveillance of the communications of organizations and individuals is a constant concern regarding the implications of exercising rights protection.

That is why analyzing the cybersecurity of human rights defenders is key to seek strategies and safeguard their physical, legal, digital and psychological protection, in order to mitigate vulnerabilities, threats and intimidation they may receive. The aforementioned collaborates with the strengthening and quality of democracy and the rule of law.

4 Resolution 53/144: United Nations Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms. Adopted by the General Assembly on December 9, 1998.

5 United Nations Human Rights Office (2019). Rights to freedom of peaceful assembly and of association. https://www.ohchr.org/. Accessed on June 04, 2024.

6 Legislative Information System of Paraguay. Bill. #Expediente: D-2164736. Draft Law for the Protection of Journalists, Communicators and Human Rights Defenders. https://silpy.congreso.gov.py/web/expediente/124598. Accessed on July 06, 2024.

Also, it is important to note that the issue of cybersecurity began to be considered by States with greater importance since early 2000, thus, the OAS, through the Inter-American Committee Against Terrorism (CICTE), approved[7] the "Adoption of a comprehensive inter-American strategy to combat threats to cybersecurity: A multidimensional and multidisciplinary approach for the creation of a cybersecurity culture". This strategy acknowledges the challenge of building cybersecurity capacities at national and regional levels, as well as fostering collaboration between the public and private sectors.

An analysis carried out by TEDIC (2016) indicates that the challenge in terms of cybersecurity is not only related to international terrorism, espionage or cybercrime, but also requires significant attention to the source code of software and hardware used, whether it be the operating system or various applications.

TYPES OF CYBERSECURITY ATTACKS

there are several types of cybersecurity attacks and new variants are constantly evolving. In Paraguay, the Cyber Incident Response Center (CERT-PY)[8] under the Ministry of Technology, Information and Communication (MITIC) has been operating since 2012[9] and records and monitors the main types of cyberattacks or incidents reported in the country[10]. The following are some of the types of attacks that occur in Paraguay and that the organization refers to:

- **System compromise:** this type of incident occurs when servers are subject to website infestation or deconfiguration, injection of malicious code or files, among others.
- **Unwanted or malicious mail (SPAM):** these correspond to unsolicited or unwanted e-mails that are sent for deceptive purposes (scam, extortion, among others).
- **Phishing:** This happens when perpetrators of cybercrimes attempt to gain the trust of individuals or organizations by using messages and arguments that create credibility, leading victims to enter their data on fraudulent websites or forms. Typically, attackers request bank details, passwords, personal information, and more.
- **Malicious software (Malware):** this is usually web-based software that runs without any explicit indication from the user and installs itself on the system. They are usually malicious downloads that can be viruses, trojans, worms, scripts, ransomware, among others.
- **Unauthorizes access to accounts, systems or data:** this type of attack occurs when the attacker gains unauthorized access to the personal or institutional account using some computerized method.
- **Scanning / Brute force:** occurs when access to the system is given through password cracking (approximation tests until the password is cracked), port scanning, among others.
- **Configuration problem/vulnerability:** this type of attack is defined by situations related to Internet that constitute a high-risk latent threat, such as the exposure of passwords, among others.

---

7 Resolution AG/RES. 2004 (XXXIV-O/04)

8 CERT/ MITIC. (2023). Report: State of Cybersecurity in Paraguay. Year 2022. https://www.cert.gov.py/wp-content/uploads/2024/01/Informe-Ciberseguridad-Paraguay-2022.pdf. Accessed on 10 May 2024.

9 SETICs Resolution No. 18/12: Which creates the Cyber Incident Response Team (CERT-PY), as a dependency of SETIC (Secretariat of Information and Communication Technologies) under the Executive Branch and signed on November 30, 2012.

10 It is important to note that CERT-PY considers not only attacks against the governmental space, but also receives information on attacks against the private sector and citizens in general.

- **Denial of services (DoS/DDoS):** occurs when a machine or website is overloaded or drowned with simultaneous requests, causing the system to collapse due to its inability to respond. This means that the website or machine is no longer available.
- **Ransomware:** this is a type of malware that infects computers or computer systems through malicious code, rendering them unusable. The perpetrators usually communicate with the victims and demand a payment to restore access to the account or website.

Other types of attacks known in the field of cyberspace include:

- **SQL injection:** this involves exploiting vulnerabilities in web applications by injecting malicious SQL code into input forms to access and manipulate databases.
- **Social engineering:** this is the psychological manipulation of people to obtain confidential or sensitive information to gain access to the system or device. This type of attack can include phishing, baiting, pretexting and tailgating. This type of attack also feeds on publicly available information, such as those found in newspapers, magazines, social media sites, among others.
- **Man-in-the-middle (MitM):** the attack occurs by intercepting communications between parties without them being aware of it.
- **Spoofing:** this attack occurs when an attacker impersonates a person or organization to gain access to information or systems. It involves spoofing IP addresses, email addresses, and/or DNS.
- **Cross-Site Scripting (XSS):** this is the use of malicious scripts on websites to attack users who visit these sites, thus stealing information and attacking on behalf of the user.
- **Rootkit:** these are tools that enable the attacker to have continuous and undetected access to a system or device.
- **Keylogger:** through software or hardware that identifies the user's keystrokes, they can steal information such as passwords and personal data.
- **Botnets:** these are networks of infected and controlled devices that can be used for DDoS, spam and other malicious attacks.

Also, on the other hand, there are certain types of cyberattacks perpetrated with the intention of generating digital violence against individuals or organizations and thus causing emotional harm. This, in turn, expands the fear that the aggressions will move from the virtual to the real world. In these types of threats, technology is used as a medium (TEDIC, 2016). It is relevant to mention some of these types of aggressions that occur in cyberspace and that undoubtedly affect cybersecurity. According to Sequera and Acuña (2023), some of these technology-facilitated gender-based violence can be[11]:

> a) Threats to physical integrity and life. b) Hate and denigrating speech. c) Extortion. d) Online defamation. e) Surveillance. f) Doxxing, g) Online harassment. h) Non-consensual dissemination of intimate images. i) Receipt of unsolicited sexual materials. j) Workplace mobbing. k) Cyber bullying. l) Coordinated attacks.

These attacks of technology-facilitated gender-based violence take place with both occasional or circumstantial frequency, as well as in a constant and prolonged manner. The occurrence of these attacks coincides with efforts to influence opinions on controversial issues, such as climate change, vaccination, sexual and reproductive health, among others.

In general, cybersecurity threats occur through social media, whether personal, professional or organizational. People normally underestimate the vulnerabilities of being online and there are various types of exposure risk, thus, one of the most common occurs when sending a friend request and try to make contact with the potential victim, the acceptance of link could help the attacker to collect a lot of information, place of work, home address, phone numbers, among other personal data. In the second stage, they use spontaneous messaging (via WhatsApp or Facebook Messenger) to request information directly from the victim (Martínez and Ávila: 217, 2021).

11 In order to know each type of violence in depth, it is recommended to read TEDIC's work on the collection and classification of cases of digital violence (cases of gender-based digital violence towards women journalists and towards women politicians). Available at www.tedic.org

CIVIL SOCIETY ORGANIZATIONS AND THEIR LEVELS OF CYBERSECURITY

it is important to know the contributions of the scientific literature and based on the evidence found as answers that organizations give or can give to the issue of cybersecurity. In this sense, Sancho (2017) systematizes documents from multilateral organizations and outlines the maturity levels in digital security that can be found in institutions and organizations (Sancho, 2017). The following describes the information:

PHASE 1

Unawareness: the organization considers digital security risk to be of little relevance and is not part of the enterprise risk management process. The organization is not aware of its level of interconnection.

PHASE 2

Fragmentation: the organization recognizes hyperconnectivity as a potential risk focus and has a limited perception of its management practices in cyberspace. The organization applies an independent approach to Internet risk with a fragmented and casual presentation of information.

FASE 3

Descendente: la máxima autoridad de la organización marca las pautas con respecto a la gestión del riesgo en Internet e inicia un abordaje de carácter descendiente de amenaza-riesgo-respuesta, sin embargo, no considera la gestión de riesgo cibernético como una ventaja medular para la organización. Phase 3: Top-down: The organization's highest authority sets the tone regarding Internet risk management and starts a top-down threat-risk-response approach, but does not consider cyber risk management as a core benefit for the organization.

PHASE 4

Mastery: the organization's highest authority is fully aware of the information regarding Internet risk management, and plans the development of policies and actions, while also defining responsibilities and reporting mechanisms. It understands the organization's vulnerabilities, its controls and its interdependencies with third parties.

PHASE 5

Interconnection: the organization is highly connected with peers and allies, sharing information and jointly mitigating risks on the Internet as part of its routine operations. Its employees demonstrate cybersecurity awareness and the organization is confident in its cybersecurity measures.

There are different options to protect the digital security of organizations. It is important to analyze how the organization operates to choose the best security measures or tools, either by building a new tool, reusing an existing one, or designing it with future reuse in mind (Bewlay et al., 2021). Collective participation in digital construction processes for civil society organizations is key to generate a strong level of protection capable of responding to possible attacks. The involvement of people is key to ensure a solid information ecosystem that will be updated by the self-interest of the community (Paes, 2024).

cybersecurity in Paraguay is an issue that needs to be socialized with stakeholders from the State, the private sector and civil society, in order to ensure transparency in the processes of regulation and implementation of digital security in the country. The State must promote participatory governance to strengthen democracy. Although there are currently monitoring centers that are recording cases of vulnerability and attacks, it is necessary to reflect on the ecosystem that makes up digital security, such as the need for a comprehensive law on the protection of personal data.

The vision of the defensive role of cybersecurity in issues related to military matters or banking processes is predominant in the country. However, it is necessary to deal with cybersecurity issues from a people-centered point of view, as the main objective, and thus provide protection and guarantee their duties and rights. This is not only a technical or national security issue. It is important, from a human rights perspective, to update the debate and propose effective and participatory mechanisms to enhance risk management in digital matters.

Regulations related to cybersecurity in Paraguay

It should be noted that progress still needs to be made in terms of cybersecurity regulations in Paraguay. Undoubtedly, one of the most necessary laws to be created is the Comprehensive Law on Personal Data Protection (Sequera, 2019). However, in recent years, some progress has been made with the approval of laws, presidential decrees and ministerial resolutions. The following are some historical-institutional milestones related to the topic, but which do not exhaust the need for more specific regulations:

- **Law № 4989/2013**, "Which creates the framework for the application of information and communication technologies in the public sector and creates the National Secretariat of Information and Communication Technologies (SENATICs[12])"[13], and then with Decree № 11.624/2013, the institution was regulated and the new governing structure for public policies for ICTs in Paraguay was established.

  It is also noteworthy that this decree created the General Directorate of ICT Policies and Development and, under its dependence, the creation of the Cyber Incident Response Center (CERT-PY), which is responsible for facilitating and promoting the protection of cyber systems and information that support the national infrastructure both governmental and private sector, as well as to provide rapid responses to cyber incidents. With the intention of achieving greater effectiveness and joining efforts from the legislative on ICTs, Decree № 5323/2016 was approved, "Whereby Arts. 20 and 21 of Law № 4989/2013 are regulated". This regulation stipulated that State Agencies and Entities should integrate the Coordination and Interoperability Committee, which was responsible for developing an annual work plan[14].

12 It should be clarified that the current governing body of ICTs in Paraguay is the Ministry of Information and Communication Technologies (MITIC). Previously, the institution had another rank: National Secretariat of Information and Communication Technologies (SENATICs) and was previously known as the Secretariat of Information and Communication Technologies (SETICs).

13 With the approval of this regulation, Law No. 8.716/2012 "Whereby the Secretariat of Information and Communication Technologies (SETICs) is created and regulated" was repealed.

14 It should be noted that one of the most sensitive areas is the one concerning children and adolescents. Thus, Law No. 5653/2016, "On the protection of children and adolescents against harmful content on the Internet" was created. This Law was then regulated by Decree №8098/2022 and, later, SENATICs Resolution №143/2017 approved the minimum technical specifications for the software mentioned in the aforementioned law. A few years later, with Resolution MITIC No. 699/2019, the "Minimum security criteria for the development and acquisition of software" was approved.

- **Law № 6,207/2018**[15], "Which creates the Ministry of Technologies, Information and Communication and establishes its organizational charter". Through this regulation, the General Directorate of Cybersecurity and Information Protection was also created within MITIC, dependent in turn on the Vice Ministry of Information and Communication Technologies. Decree № 2274/2019 regulates the aforementioned law. It is important to highlight that MITIC replaces the National Secretariat of Information and Communication Technologies (SENATICs), changing its institutional status within the hierarchy of the Executive Branch, thus, from a Secretariat to a Ministry.

- MITIC **Resolution № 346/2020** approves and implements the regulations for mandatory reporting of cybersecurity incidents by the State Agencies and Entities (OEE) to the Ministry of Information and Communication Technologies (MITIC), through the Cyber Incident Response Center (CERT-PY), under the General Directorate of Cybersecurity and Information Protection. This resolution indicates that any citizen, company, public institution or foreign organization can report a cyber incident affecting an information system of the national digital ecosystem, whether their own or that of third parties.

- **Decree № 6234/2016**[16]. "Whereby the application and use of Information and Communication Technologies (ICTs) is declared to be of national interest, the minimum structure that must be in place is defined and other provisions are established for its effective functioning". This Decree mandates that all Executive Branch institutions must have a single area specialized in Information and Communication Technology. This decree was relevant for the institutionalization and ordering of matters related to ICTs in general.

- **Decree № 7052/2017**. "Whereby the National Cybersecurity Plan is approved and the National Cybersecurity Commission is integrated". The Plan is the document that sets out the basis for considering and acting on cybersecurity matters. It states that they seek to integrate the sectors involved with ICTs to achieve greater economic growth and maximization of benefits, thus achieving a more stable, secure, reliable and resilient cyberspace.

  This decree outlined seven action points to be developed under the leadership of the Executive Branch: (i) Awareness and Culture; (ii) Research, Development and Innovation; (iii) Critical Infrastructure Protection; (iv) Response Capacity to Cyber Incidents; (v) Cybercrime Investigation and Prosecution Capacity; (vi) Public Administration; and (vii) National Cybersecurity System.

15 This law repealed Law No. 4989/13 and declared the extinction of SICOM and SENATICs respectively.

16 This decree in turn repealed Decree №1840/2014: "The application and use of Information and Communication Technologies (ICT) in public management is declared of national interest and the implementation of Specialized ICT Units in the institutions under the Executive Branch is ordered".

The National Cybersecurity Commission was also established, which is composed of the following institutions[17]:

a. Ministry of Foreign Affairs;
b. Ministry of National Defense;
c. Ministry of Interior;
d. National Police;
e. Ministry of Industry and Commerce;
f. Ministry of Education and Science;
g. National Secretariat of Information and Communication Technologies (SENATICs);
h. National Telecommunications Commission (CONATEL);
i. National Council of Science and Technology (CONACYT);
j. National Computing Center (CNC);
k. Social Security Institute (IPS);
l. Public Prosecutor's Office;
m. Judicial Branch; and
n. Legislative Branch.

- **Law № 6822/2021**, "On trust services for electronic transactions, electronic document, and electronic transferable documents". This Law establishes the legal framework for electronic identification, electronic signature, electronic seal, electronic time stamp, electronic documents, electronic files, certified electronic delivery services, website authentication certificates, electronic transferable document and in particular for electronic transactions. This Law was later regulated by Decree No. 7576 /2022.

Public Prosecutor's Office - Specialized Unit for Computer Crimes

In 2001, the Budapest Convention on Cybercrime and Internet Crimes was created, Paraguay ratified it in 2017 and began a process of harmonization with local laws and the local criminal system (Sequera and Samaniego, 2018). In Paraguay, the legal entity in charge of investigating cybercrime cases in Paraguay is the Public Prosecutor's Office, through the Specialized Unit on Cybercrimes, which was created in 2010 by FGE Resolution No. 3459/10 and expanded by FGE Resolution No. 4408/2011. They act against punishable acts committed or facilitated through technology. According to Resolutions No. 3459/10 and 4408/2011, the criminal types of exclusive competence of the Specialized Unit on Cybercrimes are the following: unauthorized access to data, interception, preparation for unauthorized access to data, alteration of data, unauthorized access to computer systems, sabotage to computer systems, alteration of relevant data, forgery of credit and debit cards and fraud through computer systems. Also, their website indicates that the institution plans to provide training on cyber bullying, sexting, child pornography and grooming.

17 The decree also states that civil society, private sector and academic organizations may be members of the National Commission and the Specialized Working Subcommittees. The National Cybersecurity Coordinator and the National Cybersecurity Commission are responsible for convening and guaranteeing the participation of these bodies.

National Government and its public policies on cybersecurity

MITIC started a process to update Paraguay's National Cybersecurity Strategy 2024-2028 (ENC PY)[18]. The government's current intention is to turn the country into a regional technological hub, which responds to the need to show digital security in order to attract investors to Paraguay. Technological upgrade concerns focus to cryptocurrency, cloud computing, and artificial intelligence. Concerns about threats refer to dealing with possible financial losses, theft of personal data, and service interruptions, among others.

In 2023, the National Government signed a cybersecurity agreement with the United States of America, the institutions in charge of leading and presenting the agreement were the General Directorate of Cybersecurity and Information Protection (DGCPI), of MITIC, and the Infrastructure Security and Cybersecurity Agency (CISA)[19]. In this sense, the agreement signed between Paraguay and the United States of America outlines the path to be followed[20] in terms of digital technology, both in infrastructure and in the promotion of Internet. It should be noted that digital defense is one of the key points to be addressed by the agreement.

Cyber incident reporting

According to the latest publication of the CIRT-PY (2022), the statistics on the latest cyber incidents in the country, which were reported by State institutions, foreign CSIRTs, private sector companies and citizens, show that 3,668 incident reports were received and the institution managed to deal with 2,083 of these cases. The report indicates that most of these events involve compromised systems or devices (defacement), servers with malicious code and phishing. Meanwhile, ransomware incidents, although less frequent, still occur.

The vulnerabilities identified are related to weak passwords, outdated passwords and also to malware being part of Botnets (Emotet, Avalanche, Hajime botnet). The document also states that they had no records of DoS/DDoS attacks, but they indicate that, in general, when this type of case occurs, the victims prefer to report directly to the Internet service providers. The same happens with unauthorized access to accounts or data, which victims prefer to contact directly with the service platforms, be it Google, Facebook or X, among others. This situation shows that there is a need to expand and unify the system for recording cyber incidents in the country.

18 Ministry of Technologies, Information and Communication (June 6, 2024). Why it is important for Paraguay to update its National Cybersecurity Strategy. https://mitic.gov.py/por-que-es-importante-para-el-paraguay-actualizar-su-estrategia-nacional-de-ciberseguridad/. Accessed on June 12, 2024.

19 Diario La Nación. (2023). Paraguayan cybersecurity milestone highlighted after cooperation agreement with the US. www.lanacion.com.py/politica/2023/07/06/destacan-hito-en-ciberseguridad-paraguaya-tras-acuerdo-de-cooperacion-con-ee-uu/. Accessed on 13 June 2024.

20 Diario ABC Color. (2023). Paraguay signs cybersecurity agreement with the US. www.abc.com.py/politica/2023/11/11/paraguay-firma-con-eeuu-acuerdo-de-ciberseguridad/. Accessed on 26 May, 2024.

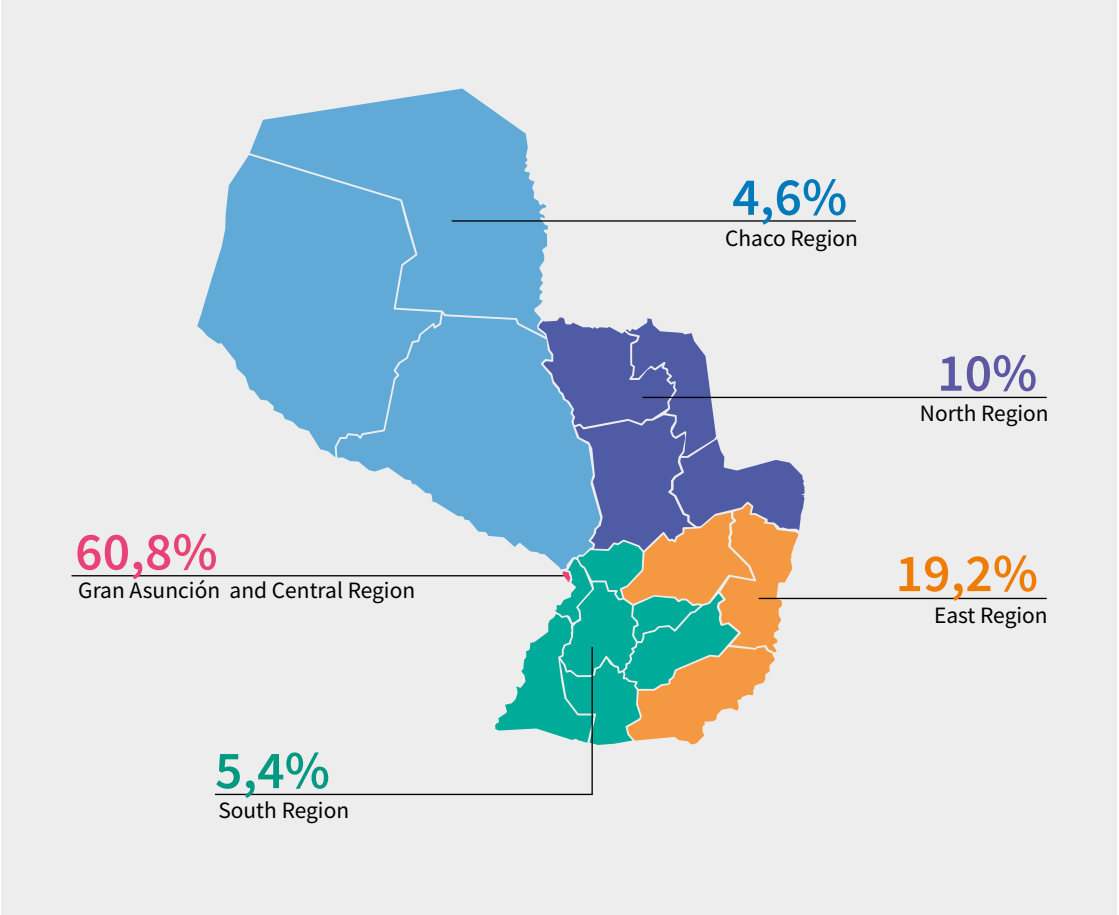
QUANTITATIVE FINDINGS

The survey collected information from one hundred and thirty (130) human rights defenders in Paraguay. The survey sections focused on information related to: a. demographics, b. location and mobility, c. infrastructure and digital tools, d. security, e. risks and threats, and f. gender-based violence. The organizational affiliation of defenders was varied, as they stated that they belonged to peasant, indigenous, urban, environmental, health, children and adolescents, freedom of speech, feminist, LGTBIQ+, youth, and student organizations, among others.

A. SOCIODEMOGRAPHIC DATA

the age range of participants was: 31.5% were between 18 and 28 years of age; 36.9% were between 29 and 45 years of age; 25.4% were between 46 and 60 years of age and 6.2% were between 60 and older, respectively. Most of the people surveyed live in Gran Asunción and Central Region (60.8%); in the Eastern Region (Caaguazú, Itapúa, Alto Paraná and Canindeyú) live 19.2% of them; in the Northern Region (Amambay, Concepción, Canindeyú and San Pedro) 10%; in the Southern Region (Cordillera, Guairá, Caazapá, Misiones, Paraguarí, Central and Ñeembucú) 5.4%; in the Chaco Region (Alto Paraguay, Boquerón and Presidente Hayes) 4.6% respectively.

GRAPH 1. Area of residence of the surveyed defenders.



*Observation: Based on one hundred and thirty (130) respondents.

Regarding the level of education, the survey sample shows that 0.8% of the people surveyed have no schooling; 4.6% have completed elementary school; 16.9% have completed high school; 10.8% have completed a university degree; 57.4% have an undergraduate degree; and 23.1% are professionals with a postgraduate degree.

The percentages on the preferences for receiving or following learning instructions or suggestions were very close, showing small variations. Most of the participants indicated that when receiving instructions or learning suggestions they feel more comfortable following instructions with a step-by-step image guide (37.7%); in second place, they prefer to follow instructions from a written document (36.9%); and, lastly, they indicated that they find it better to follow instructions from a video (25.4%).

Respondents identified themselves mostly as Latinos, accounting for 42.3%; followed by mestizos, 34.6%; then as whites, 7.7%; as indigenous, 6.9%; and 0.8% as Afro-descendants. Significantly, 7.7% said they did not feel identified with any of the above.

When asked if the persons surveyed had any type of disability, 95.4% said they did not and 4.6% said they did. Of the latter group, the most frequent disabilities were visual (50%), followed by hearing, physical and psychosocial disabilities (16.7% each).

Regarding gender identity, 61.5% of the respondents identified themselves as women; 35.4% as men; 2.3% as non-binary; 0.8% as trans men. While the question on sexual orientation showed the following result: 62.3% said they were heterosexual persons; 20% as bisexual persons; 6.9% as homosexual persons; 1.6% as asexual (hetero-affective and demisexual); 1.5% as pansexual persons; and 7.7% did not want to share this information.

B. LOCATION AND MOBILITY

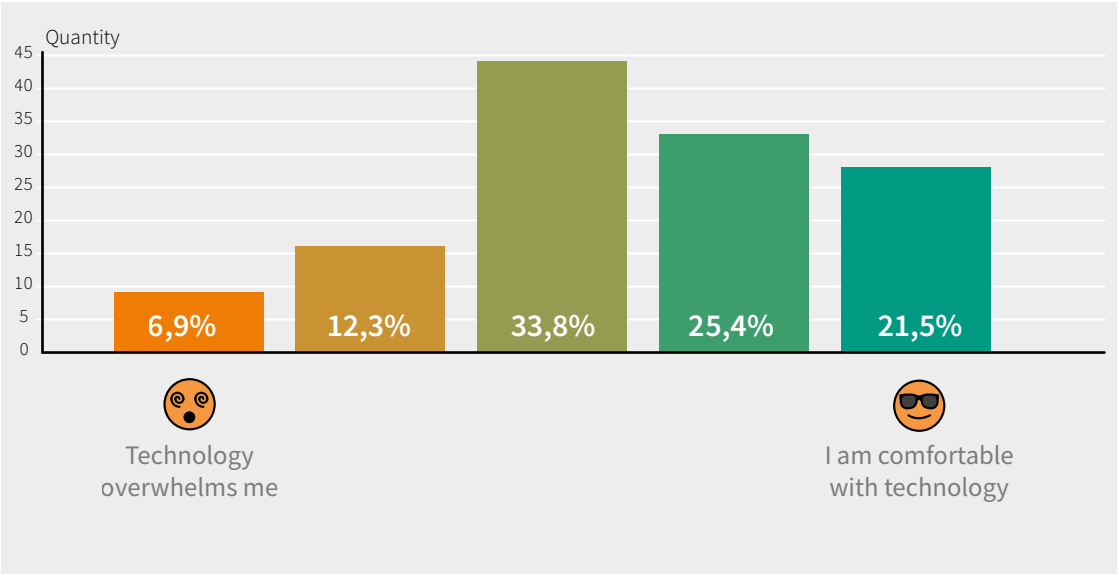
when asked about where they live, 53.8% of the respondents indicated that they live in the capital, 23.1% in a municipal capital, and 23.1% in rural areas. When asked in what type of area they work, 60.8% mentioned that they work in departmental capitals, 26.2% in rural areas and 13.1% in municipal capitals/cities.

Respondents indicated that they travel outside their cities and/or neighborhoods where they live with the following frequencies: 34.6% travel weekly; 33.8% daily; 26.9% monthly; 2.3% annually and 2.3% do not travel at all.

C. INFRASTRUCTURE AND DIGITAL TOOLS

when asked about their feelings on the use of digital technologies, people rated themselves using a scale of 1 to 5, where 1 represented "Technology overwhelms me" and 5 "I feel comfortable with technology (I install and test tools and I have security measures in my accounts). Most people agreed that they are in an intermediate degree, i.e. with 33.8% in rank 3. Following this, 25.4% rated themselves in rank 4, and 21.5% rated in 5. In the case of rank 1, where the person mainly feels overwhelmed by technology, a group of 6.9% was recorded, while rank 2 reached 12.3%.

GRAPH 2. Identification in relation to the use of technology*.



Observation: Ranks near 1 represented "Technology overwhelms me" and those near 5 "I am comfortable with technology (I install and test tools and have security measures in my accounts)".

Regarding the use of digital technologies, 63.1% mentioned that they use the technology autonomously; 23.1% indicated that they consult with someone at work or a support network; and 13.8% stated that they always consult with a family member or close friend.

The activities they perform through digital technologies are mostly for education and work purposes (participate in virtual meetings for their work or training processes) at 85.4%; for entertainment and communication purposes (access social media and spontaneous messaging) they coincided at 70%; and for digital advocacy purposes (develop a political or social agenda through digital media), they do so at 27.7%.

When selecting the devices they use for their daily activities, defenders indicated 99.2% of coincidence that the smartphone is the main device used; in second place, laptops (76.9%); in third place, with 18.5%, desktop computers and USB memory; in fourth place, external hard drive (16.2%), in fifth place, tablets (13.8%); in sixth place, smart watches or similar (7.7%); and finally, voice assistant (6.9%).

People distinguished the options on how they connect to the internet, 76.9% indicated that the most common way is through personal data; 71.5% indicated that they do it through home internet; 53.1% through internet at work; 20% through a private WIFI point; 13.8% through data provided by work; 2.3% through data provided by some international cooperation; 11.5% through public internet (in parks or libraries, etc.); 8.5% in an Internet café; 6.3% with a prepaid system.

A majority of 98.5% of defenders reported that they have a phone signal for their daily activities, as opposed to the 1.5% who do not.

The defenders indicated that they use the following types of tools for work activities: 116 people use personal email accounts; 104 defenders communicate through instant messaging apps (WhatsApp, etc.); 97 people use cloud storage tools; 90 people use social media accounts; 70 defenders prefer email accounts exclusively for work; 21 have security software (antivirus, circumvention tools, etc.); 19 use live streaming; 2 use support software for various capacities; and 4 people stated other types of activities.

In the section related to social media, people selected under multiple choice criteria which social media they use. Their answers showed that they use Facebook at 86.2%; Instagram at 76.9%; Twitter at 62.3%; TikTok at 38.5%; Snapchat at 6.2%; and, finally, a cumulative 6.4% indicated other types of platforms (LinkedIn, Pinterest, etc.).

Respondents indicated that their main instant messaging tool is WhatsApp (100%), then Facebook Messenger (41.5%), Telegram (41.6%); followed by Signal (12.3%), and, finally, (1.6%) mentioned another type of messaging (Outlook chat and Instagram chat). In a next field of inquiry about other type of social media they use, people indicated Instagram, LinkedIn, Tinder, Slack, Reddit, Tumblr and iMessage.

Regarding live streaming, people said they use Facebook Live (42.4%), Instagram Live (42.4%), Twitter Spaces (5.4%), Twtich (4.3%), and YouTube Live (17.4%).

Of the people surveyed, 54.6% indicated that they manage social media, websites or any other digital service for the organization in which they work, in contrast, 45.4% do not. People from the first group mentioned that they manage social media (Instagram, X, Facebook, TikTok), websites and Web Apps, as well as the organization's WhatsApp account.

On the section that inquired about the operating system they have on their computers, 44.6% mentioned that they use legally acquired Windows; 18.5% pirated or unlicensed Windows; 29.2% indicated that they use Windows, but do not know if it is legal or not; 5.4% use Mac iOS X (Apple); 4.6% GNU/Linux (Free Software); and 11.7% do not know the name of the operating system they use.

The majority of the defenders, 97.1%, use smartphones as their communication device; 11.5% also use landline phones; 3.8% said they use satellite phones; and 0.8% mentioned tablets.

When asked about the operating system of their smartphones, people said Android System (80%); iPhone iOS (17.7%); Windows Phone 0.8% and others at 2.4%.

The means of communication they use most for work are WhatsApp (96.9%); E-mail (75.4%); Phone calls from smartphones (60.8%); Google Meet (41.5%); In-person conversations (34.6%); Zoom (16.9%); Facebook or Messenger (13.1%); Teams (7.7%); Calls from landline (4.6%); Twitter (4.6%); SMS (2.3%); Skype (1.5%) and others (2.4%).

D. SECURITY

A high percentage of respondents, 76.2%, indicated that they had not received any training in digital security, as opposed to 23.8% who had received some training. Those who said they had received some training, added that they did so before or during the pandemic, another smaller group did so recently within the last year.

On the section that addressed whether the person has conducted any digital security risk analysis, 91.5% said that they had not done so, as opposed to the 8.5% who said that they had. Of this last group, some mentioned that their last analysis was in 2021, and then 2023. One comment stands out that mentioned "I do it all the time, but I need to take security actions".

The percentage of people who use the same password for more than one account is 56.2% as opposed to 43.8% who use different passwords for their accounts. When asked if their accounts open automatically when they log into the browser without asking for passwords, 70% said yes.

When asked if they share their digital devices, 84.6% said they do not, while 15.4% mentioned that they do. And, on the contrary, when asked if they borrow devices from others, 79.2% said that they do not and 20.8% that they do. People who share devices in both groups indicated that they share home and work desktop computers, notebooks, tablets and smartphones.

52.3% indicated that they have a backup copy of the information stored on their devices; 21.5% said they do not have a backup copy and 26.2% said they do not know.

Regarding the security measures adopted by the defenders, 88.5% indicated that they have a password on their phones (e.g. password, pin, pattern or fingerprint); 65.4% said they have a password on their other devices such as computers or tablets (e.g. password, pin, pattern or fingerprint); 37.7% use antivirus on their computer or tablet; 16.2% use antivirus on their smartphone; 0.8% VPN or authenticator; 3.8% none; and others 1.6%.

Also, HR defenders said that they always log out when they finish using a device that does not belong to them (74.6%); use different passwords for all their accounts (34.6%); use two-step authentication (40.8%); store their passwords in a secure place or in a password management program (e.g. KeePass, 1Password, BitWarden, etc.) (11.5%); they encrypt the content of their devices (9.2%); they regularly delete sensitive data (e.g., messages, photos, etc.) from their devices (e.g., phone, laptop, tablet) (40.8%); regularly review the security and privacy settings of their accounts and devices (16.2%); back up data to external storage such as external hard drives, USB drives (15.4%); back up to the cloud (e.g. iCloud, Google Drive, Microsoft OneDrive) (35.4%); none (7.7%); while 3.2% mentioned other types of practices, such as deleting sensitive data but not regularly; working in the cloud (Google drive) and using different work accounts; having different accounts for different activities; browsing incognito and also that they randomly and non-systematically use different types of security.

When asked about the security measures they use to protect their WIFI network, 70.8% stated that they use strong passwords; 10.8% change the password of the WIFI network periodically; 3.1% stated that they create a guest network different from the one for their own use and 20.5% stated that they do not use any security measures.

E. RISKS AND THREATS

94.6% of the people surveyed said that the organization in which they work does not have any security protocol to address risk situations or digital threats, only 5.4% said that they do have protocols and detailed that among the actions considered by the protocols, the following points stand out: communicate the incident to the IT focal point; do not open suspicious links; activate VPN when accessing an App of the organization; criteria for password use (length and characters, as well as periodic change); among others. The percentage values of security incident records indicate that 94.6% said that they do not have a record of digital security incidents.

GRAPH 3. Availability of digital security protocols in organizations.

The organization does not have a protocol on digital security

The organization has a protocol on digital security

It is important to note that people indicated that both the protocol and the recording of digital security incidents in the organization generally falls under the responsibility of the IT and/or communication team, while the other members are not aware of the procedures.

Regarding the identification of the most immediate and serious digital threats that defenders perceive as potential risks they may be facing personally or organizationally, they selected the following options:

Unauthorized access (hacking) to email or social media accounts.	**63,1%**
Phishing: links to fake sites via text messages, instant messaging or email, in order to steal personal information and login information, or install malicious programs.	**43,1%**
Loss of information	**32,3%**
Sexual harassment through social media, email, calls or text messages.	**24,6%**
Theft of devices (smartphones, computers, tablets, hard drives, USB).	**30%**
Harassment through social media, email, calls or text messages.	**18,5%**
Deletion of information on the organization's website or third-party platforms where information is stored.	**16,2%**
Hijacking of the organization's information for extortive purposes (Ransomware)	**12,3%**
Confiscation of devices by authorities (e.g. Police, Army, Prosecutor's Office).	**14,6%**
Unauthorized access (hacking) to the organization's web page.	**13,1%**
Bullying or harassment through social media, email, calls or text messages.	**9,2%**
I do not believe I am facing any threat.	**9,2%**
Alteration of information on the organization's website or third-party platforms where information is stored.	**8,5%**
Retention of devices by illegal groups (e.g. criminal gangs, drug traffickers).	**7,7%**
Other situations. People indicated that they are concerned about receiving calls without knowing how they got their phone numbers, they mentioned that they constantly receive friend requests from strange profiles, generally military personnel with foreign appearance, among others.	**2,4%**

To the question: In the last year, have you, any person in your organization or your organization suffered any digital security incident?[21] 58.5% indicated that they have not suffered any digital incident, while 41.5% indicated that they have. From the latter group, people selected the following types of attacks received:

Unauthorized access (hacking) to email or social media accounts	**38,9%**
Phishing: links to fake sites via text messages, instant messaging or email, in order to steal personal information and login information, or install malicious programs.	**24,1%**
Impersonation calls or messages through social media, text messages and calls with the purpose of scamming, stealing personal information and access information.	**22,2%**
Tapping (interception of communications, voice calls and messages).	**20,4%**
Theft of devices (smartphones, computers, tablets, hard disks, USB devices, etc.).	**18,5%**
Loss of information.	**16,7%**
Harassment through social media, email, calls or text messages.	**14,8%**
Sexual harassment through social media, email, calls or text messages.	**13%**
Unauthorized access (hacking) to the organization's web page.	**9.3%**
Deletion of information on the organization's website or third-party platforms where information is stored.	**7,4%**
Bullying or harassment through social media, email, calls or text messages.	**5,6%**
Hijacking of the organization's information for extortive purposes (Ransomware).	**1,9%**
Alteration of information on the organization's website or third-party platforms where information is stored.	**1,9%**
Confiscation of devices by authorities (e.g. Police, Army, Prosecutor's Office).	**1,9%**
Retention of devices by illegal groups (e.g. criminal gangs, drug traffickers).	**1,9%**
Other types of incidents. In this category, people mentioned cases such as turning on the camera and recording without manipulating it, and the constant creation of fake profiles.	**3,8%**

21 This question was enriched by clarifying that an incident occurs when the security of your services, infrastructure or information has been compromised or breached.

When asked if they filed a complaint regarding the incident, 77.8% said that they did not file a complaint, as opposed to 22.2% who did file a complaint. Those who did report the incident mostly reported it to social media platforms (Google, Facebook, WhatsApp) (70.8%), secondly to the police (29.2%) and finally to international institutions (4.2%). They described that the type of responses they received from institutions were generally marked by a lack of results and a lot of bureaucracy. Some people said that their experience was limited to the institution receiving the complaint. Here are some illustrative phrases:

- *I contacted META and followed the steps that a Facebook assistant instructed me to follow, but we were unable to recover our Facebook page as the process became very bureaucratic and time consuming.*
- *In addition to the lengthy response time, the referral to a specialized technical group for further bureaucratic processes was the reason why we dropped the reporting.*
- *I did not file a complaint; I just made a statement saying that my WhatsApp has been hacked and that I am changing my number.*
- *I received the support of my friends and some people who work in community radio stations.*
- *It was not my case; it was the case of colleagues from other offices in the network. The global IT team took action and communicated the case to all staff in Latin America and the Caribbean, giving security recommendations.*

People reported that their jobs were not affected by the incidents at 68.5%, as opposed to 31.5% who said they had been affected.

Also, people indicated that in case of suffering a digital security incident they would immediately turn to: other organizations (47.7%); family members (35.4%); institutions (Ombudsman's Office, cooperation entities) (30%); specifically, to police institutions (26.9%); the community (24.6%); they would not turn to anyone (11.5%); international institutions (6.9%); and the church (1.5%).

People were asked if in the last year, any person in their organization or their organization has experienced any threat through mail, messages on social media, WhatsApp, text messages and/or phone calls due to their activities[22], 73.1% said no and 26.9% said yes. Likewise, they were asked if they have been exposed to direct threats involving access to personal and sensitive information about them[23], 73.8% said no and 26.2% said yes. In this last group, when asked if their work has been affected by these situations, 80.5% said no and 19.5% said yes.

22 This item clarified that threats include threats of a sexual nature, threats of death or other physical harm, threats or intimidation of close family members, etc.

23 This item clarified that personal and sensitive information includes contact information, location, information about threats or ongoing legal proceedings, information about political interests, etc.

People gave references on how security could be improved and observations on dangerous practices that could jeopardize the security of the organization. They said that they usually activate the "Airplane Mode" when they start a meeting to discuss sensitive information while, mostly, they indicated that they need training on the subject of digital security, as a lack of knowledge sometimes leads them to overlook or fail to recognize potential threats or risks. They mentioned that there is a need to generate digital security protocols, as well as campaigns to ensure that communication is free and unmonitored.

The people identified risks for defenders and organizations, mentioning that one of the biggest risks they face is the loss of information, lack of backup, how to avoid phishing attacks, how to deal with fake profiles, and how to take care of defenders according to their level of exposure.

Some people elaborated on specific situations:

- *A person from the organization who manages the social media of the organization traveled to Europe for an event and did not have digital security information, that caused him not to identify risk situations in the use of any public WIFI and connection to USB ports at airports, which resulted in the hacking of our social media through a virus.*

- *I have noticed that during protests for the Tariff 0 and HC Law, my colleagues and family members received threats from the public institution (university) of which I am a student.*

- *My mistake is to use free WIFI in situations where I don't have the possibility to have data.*

- *It is important that our HR defenders network organizes a series of workshops to analyze and establish strategies, actions and mechanisms for digital security for defenders and their organizations.*

When people were asked if they want to know more about information security and technological infrastructure to perform their work better without fear of making mistakes, they said that they need workshops or courses to improve personal, professional and organizational security. They said that it is a priority to start these trainings to prevent situations before regretting consummated facts. Some people described the need as follows:

- *From the student organization it would be ideal to know in depth about reliable tools to protect our data or files. Additionally, understanding the probability of "hacking" or "tapping" of mobile devices when we are in contexts of struggle or actions involving force, such as takeovers, protests, demonstrations, etc.*

- *We need to learn how to secure accounts and websites of organizations more effectively.*

- *We want to securely store personal information within the clouds and devices, and to know if there are laws regarding leaked information or threats received from the authorities.*

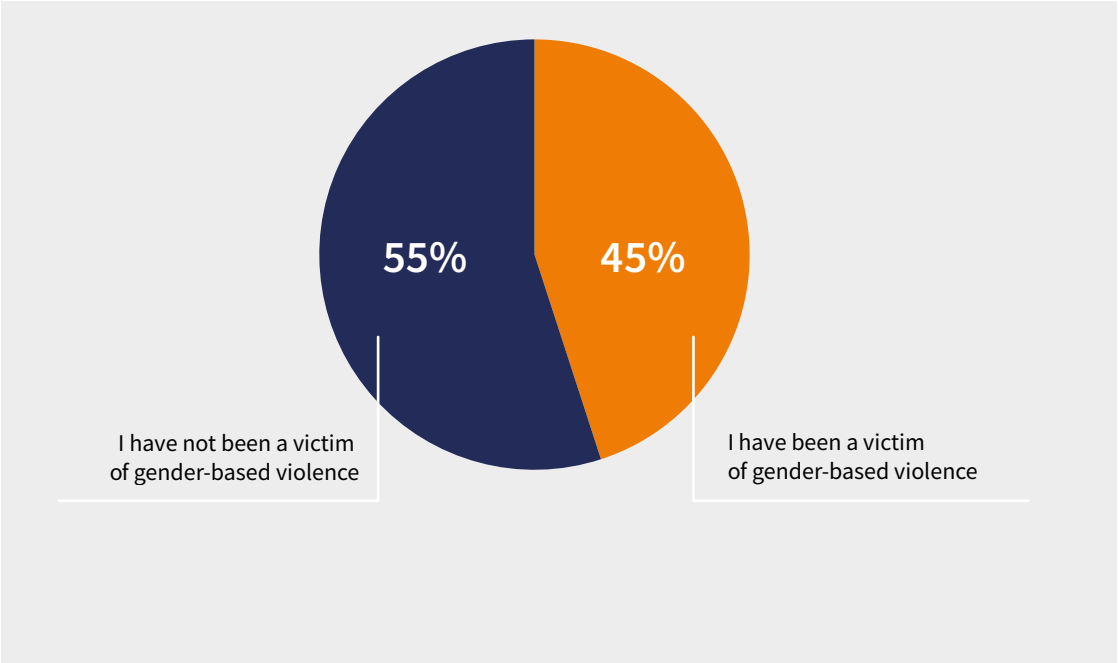
- *We need help to better understand technology.*

- *How can we detect breaches and protect websites.*
- *Training on how to use our phones.*
- *Tips to elaborate the protocol.*
- *Many times, we do not open emails when they look suspicious or we sometimes detect that an attempt was made to access the organization's Gmail. We need more support in digital security.*
- *We want training on digital security issues for human rights activists of children and adolescents.*
- *We need to better understand encryption and understand how device monitoring occurs.*

F. GENDER-BASED VIOLENCE

out of those surveyed, 45.4% said that they had been victims of some form of gender-based violence and 54.6% said that they had not. Specifically, 40% said they had been victims of some form of gender-based violence through digital media, while 60% said they had not.

GRAPH 4. Cases of gender-based violence against women human rights defenders in Paraguay.



When asked about the form of gender-based violence facilitated by technology of which they have been a victim, the following options were mentioned:

Cyberbullying.	21,6%
Discrimination (Unfavorable or harmful treatment given to a person for arbitrary reasons based on gender, sex or sexual orientation).	21,6%
Sexual harassment through social media, email, calls or text messages for arbitrary reasons based on gender, sex or sexual orientation.	15,7%
Sexual offense (verbal, non-verbal and written expressions).	13,7%
Disclosure of personal information such as: address, phone number, social media, work address, among others (doxxing) for arbitrary reasons based on gender or sexual orientation.	9,8%
Bullying or harassment through social media, email, calls or text messages for arbitrary reasons based on gender, sex or sexual orientation.	5,9%
Online identity theft.	3,9%
Non-consensual disclosure of intimate images.	3,9%
Sextortion (blackmail or extortion with an image or video of the person naked or performing sexual acts).	2%
Another form of digital gender-based violence.	2%

Specifically, when asked about other forms of technology-facilitated gender-based violence they received, people reported having received: death threats; inferior treatment because they are women; and offenses in social media. According to them, attacks based on sexual orientation and the disclosure of sensitive information are common situations.

When asked about the actions needed to reduce gender-based violence in virtual spaces, the defenders said that: it is necessary to regulate the issue of digital security with an approach that fights against discrimination and racism, to have a State present, to generate public policies for data protection, to promote education and training on digital matters to learn and practice mechanisms for personal and organizational care, and to demand that social media platforms strengthen their security mechanisms. They propose to think about what can be done with fake profiles, as it is a concern since the highest level of harassment comes from this type of accounts. They consider that there is a need to raise awareness with the police and the judiciary so that they understand the exposure of human rights defenders in the face of so much hate speech and harassment, among other types of violence. The following are some of the contributions made by human rights defenders:

- *There is a need for education on digital security and on not publishing information that can be used and turned against us. I think the levels of exposure we are reaching is high and we are giving away our information and we should set limits.*

- *Violence needs to be brought to light and be sanctioned.*

- *The truth is that violence should be sanctioned, I believe that impunity fostered by false identities is a breeding ground for violent people. On the other hand, it is structurally necessary to educate.*

QUALITATIVE FINDINGS

CONSIDERATIONS ON THE QUALITATIVE APPROACH

the qualitative approach was based mainly on the use of focus groups and semi-structured individual interviews based on guidelines and questionnaires[24].

Two (2) focus groups were conducted with the participation of 8 people per group. The participants were defenders from organizations working on different human rights issues (right to the city, peasants, LGTBIQ+, education, environment, among others). Three (3) in-depth interviews were also conducted with key informants due to their experience in cybersecurity and/or human rights.

The dynamics of the qualitative approach made it possible for the participants to freely elaborate responses based on questions and situations proposed by the interviewer, producing a frame of reference that allowed inquiring about the consensus and disruptions during the conversations.

The results are presented on the basis of themes with general and particular findings, taking into account age groups, actors and geographical areas of action. The phrases and verbalizations that illustrate the findings of the groups and interviews comply with the principle of anonymity.

Profiles of cases interviewed

	Code	Profile	Characteristics
FOCUS GROUPS	G1DJ	HR Defenders Young people From 18 -30	8 participants: 4 women 4 men Defenders of women, youth, LGTBIQ+, environmental and other organizations.
	G2DA	HR Defenders Adults From 34 -55 years old	8 participants: 4 women 4 men Defenders of peasant organizations, education, culture, environment, etc.
INTERVIEWS	E1	HR Defender	Defender working on children and adolescents matters More than 5 years of experience in the field of human rights
	E2	HR Defender	Defender of peasants' rights More than 5 years of experience in the field of human rights
	E3	HR Defender	Director of a HR organization. More than 5 years of experience in the field of human rights

24 The guidelines were developed by Fundación Karisma and were adapted and adjusted for application in Paraguay.

MAIN FINDINGS

1. Fields of action of Human Rights defenders

Human rights defenders distinguish their areas of action as institutional and from the perspective of citizens and at national and local levels. At the institutional level, they participate in discussions on regulatory frameworks, working groups with the Executive Branch, public hearings and lobbying with the legislature and accompanying the defense of cases in the Courts. On the other hand, within civic networks, they develop projects, workshops, agendas for citizen participation and promotion of human rights. It is worth mentioning that most of the people interviewed agree that, in recent years, there have been setbacks in both spaces, as there has been a rise in groups that attack fundamental human rights, especially the rights of groups such as women and LGTBIQ+ people.

These anti-rights groups have great dissemination capacity and resources to disinform and be visible through social media and digital platforms.

- *W: I have been working for more than two decades in technical meetings with representatives of the Ministry of Health and Education, and it is impressive how the directors themselves are afraid to talk about women's rights or LGTBIQ+, and the word gender is already banned.*

- *M: It's exactly like that, this is because the anti-rights groups managed to infiltrate, disinform, manipulate, invent stories that make people afraid and sow hatred in the communities. (G2DA Adult Human Rights Defender, 30 to 55 years old).*

- *M: To avoid mentioning homosexuality in formal meetings, many people say they have a gender tendency and sometimes they are silent because of fear... when there are people with certain positions and who exercise power... many people do not want to speak or give their opinion because of this (E1- Defender of Children and Adolescents Rights).*

2. Dynamics of digital tools and internet use

the use of digital tools is a daily practice for human rights defenders. They consider that their use was enhanced and normalized during the pandemic. The incorporation of these tools in the dynamics of organizations and social collectives was very sudden, without the possibility of reflecting on their scope or risks.

- *W: It was like a whirlwind, there was no time to think about what we were using or the risks involved. We had to use tools for work, for meetings, like Meet, Zoom, WhatsApp groups, it's like something that came to stay, and we learned its basic use but we do not have a real knowledge of what it implies, it's learning how to use it and that's it (G2DA Adult Human Rights Defender, 30 to 55 years old).*

Most of the people value the importance of digital tools for accessing information, maintaining links, opening new training opportunities and, above all, exchanging experiences with diverse groups and collectives. In this sense, young defenders expressed that their interest in human rights activism originated in virtual spaces and online groups.

- *M: First, I followed a program of the organization (XXX) that had an influencer, and I started to get interested in deforestation, then they held a virtual conversation, and later I joined a Telegram group... Then there was a camp and now, look, I am already a volunteer for the project (XXX). I think that for young people it's a good way to get involved through social media, especially to create interest, it's difficult to just go to a meeting without knowing anything on the subject... It's like you get to know the issues, the organization little by little (G1DJ Human Rights Defender, Young people, 18-30).*

- *W: In my case, I also saw an Instagram post about an activity of the LGTBIQ+ community, I wrote a message and started to follow the account... I agree with what he says, it's not all for flirting purposes (laughs)... You can get informed, see that there are people who have the same interests, the importance of rights, and above all to discuss and participate, even more when the haters start to attack (G1DJ Human Rights Defender, Young people, 18 -30).*

- *W: Some farmers' organizations that have access to the Internet and digital tools were able to readapt strategies for marketing their products, or else they have joined forces with other organizations to create new online sales circuits.*

- *M: As a result of a project, we were able to offer the products on a web page and in WhatsApp groups, and I think that was very important to have another possibility to market the products (G2DA Human Rights Defender Adults, 30 to 55 years old).*

3. Cybersecurity

Most of the people interviewed agree that cybersecurity is still an unknown and distant topic, in the sense of incorporating it into the organizational culture. In other words, it is not consciously incorporated as part of the safeguard, protection and security practices of organizations. In this regard, they consider that the need for such an approach emerges in the face of certain political situations or events, leading to reactive responses. Greater care or perception of the risks of digital violence is more commonly felt on a personal level. In this sense, they agree on the dimension of the current exposure and vulnerability of defenders and the tension generated by publicly maintaining positions, statements or acts.

- *M: I think we are not aware of everything that the digital world means... especially for those of us who are not digital natives... We are not aware of the series of "acceptances" we give when using applications or whatever... (E1- Defender of Children and Adolescents Rights).*

- *W: For example, when the famous donation from the European community and educational transformation was being discussed, we realized how vulnerable we were in terms of communication, protection of our accounts, and data. The campaign against us was fierce... a lot of hate speech, attacks, and viral fake information with our logos (E2- Defender of Children and Adolescents Rights).*

- *M: Before any protest, we already know that we have to take care of our phones, especially those of the organization, and also of the main spokespersons (G1DJ Human Rights Defender, Young people, 18-30).*

- *W: The anti-rights campaign was very dirty... they made flyers and tried to make fun of our identities... for us it was not an offense what they said, but it was a mockery of ideological identity, gender identity, all identities. We experienced this when topics such as Educational Transformation, "UNA no te Calles", Childhood Plan... (E1- Defender of Children and Adolescents Rights).*

- *W: When we did a seminar through the Zoom platform, with open links without prior registration, they hacked into the meetings, showing porn videos or drawing on the screen... As a result of what happened, we took protective measures and made prior registrations (G2DA Adult Human Rights Defender, 30 to 55 years old).*

- *M: What is complicated is when solidarity collections are made, and scammers enter using or cloning the social media, so we look for mechanisms to guarantee information and transparency (G2DA Adult Human Rights Defender, 30 to 55 years old).*

- *One of the weaknesses pointed out by defenders is the assignment of cybersecurity care and protection matters in organizations to communication staff, as an isolated issue, almost as a technical matter to be addressed specifically. Also, the multi-tasking assignments result in the neglect of the cybersecurity of organizations.*

- *W: In most of the organizations, we are everything... community manager, spokesperson, logistics, technology manager... we do everything (G1DJ Human Rights Defender, Young women, 18-30).*

- *M: The truth is that the person in charge of social media and our website is the one in charge of communication... the rest of us don't know much about digital safety practices (G2DA Human Rights Defender of Adults, 30 to 55 years old).*

4. Repertoires of violence

Participants in groups and interviews coincide in characterizing digital violence in social media as the most frequent, on the rise and psychologically affecting human rights defenders and activists. They express concern about the fact that this situation is currently normalized. They consider that there is an unspoken perception that "one must be prepared to endure or adapt to such violence".

- *W: Violence is the social media, it's day by day and more so when agendas are installed, which sometimes are more smoke screens of the government... But it generates conversation, the hate and aggression are amazing, but the most terrible thing is that as it's already normalized, they tell you "Well, you're dealing with human rights issues" we have to expect this, we have to put up with this and it doesn't seem right to me. Something has to be done about it (G2DA Adult Human Rights Defender, 30 to 55 years old).*

- *W: As for the defamatory attacks, they have been broader attacks... this has happened to all the directors of the organization (XXX), attacks that even came from journalists... these attacks are received by all the organizations. The identification of situations of attacks occurs especially when the debates are more heated... such as the educational transformation (E3 director of a human rights organization).*

- *M: I feel safe when they don't attack me... when they don't discriminate against you, when they make comments, whether you like it or not, it has an effect on you and it affects your self-esteem (G1DJ Human Rights Defender, Young people, 18-30).*

- *W: I used to care about the aggressive and negative comments... I used to think: why people are mean to me if I am a good person... but now I don't care anymore... there is always hate in social media... and the arguments are always repeated... (G1DJ Human Rights Defender, Young, 18 -30).*

- *W: Violence is direct in comments... every time a news item comes out about me, transphobes come out... they say that I have to go to the urologist and those things... for me it's aggressive... I used to respond to comments... but then I stopped responding... people come in and wish you were dead and they don't even know what I do, what I do for a living (G1DJ Human Rights Defender, Young, 18 -30).*

Defenders perceive an increase in violence in open and specific WhatsApp groups, due to the ease with which fake information circulates. This generates heightened stances that can lead to offline violence, especially when these groups include well-known participants or who are geographically close.

- *M: The family or neighbors' groups are the most intense, I am really afraid that a situation may arise from there and that they might later want to physically attack me (G1DJ Human Rights Defender, Young people, 18-30).*

- *M: In large WhatsApp groups there are infiltrated people... who are in the groups for the broader causes.... But there's all kinds of people there... those people make fun of the arguments of defenders... those people bring false information into the group (E1- Defender of Children and Adolescents Rights).*

- *W: They are manipulative arguments... every day they attack you more... and people in the groups see and believe anything, when you realize that it is a deceptive video, but when you want to respond, they are all offended, and then "Ekyhyje chugui kuera eikoro pe callere... because ha'ekuera oimoa nde ha'eha abortera, pe'a que amoa"* [25] *(G1DJ Human Rights Defender, Young people, 18 -30).*

- *M: A situation that surprised me is that we were organizing a very important meeting for a case we were handling... and we agreed to meet at a specific place... and suddenly many police officers appeared casually in the place where we had to meet with the people affected by the violation of their rights (E1- Defender of Children and Adolescents Rights).*

25 Translation from Guarani: you are afraid of them when you walk in the streets because they think you are an abortionist, this or that.

5. Threats: risk perception

The main risk perceived refers to the public social media accounts and online articulation platforms of the organizations. These can be subject to attacks, misuse of the collective identity, mass aggressive comments and even hacking to remove them during public debate.

- *M: It's like we are now all suspects for belonging to civil society, for speaking about children's rights, rights of people with disabilities... they attack two types of profiles: -that of the organization itself and -that of the defenders (E1- Defender of Children and Adolescents Rights).*

- *W: Receiving threats... we usually ask ourselves where did they get that from... who told them... they threaten you when they expose your identity... the defender's face, they use the logo of the organization, the name... everything... the attacks mostly come from anonymous places... (G1DJ Human Rights Defenders, Young people, 18 -30).*

- *M: As an organization, we received several attacks to our servers... we had to change the server we had hired for a more secure one... and in the last three months, we received an attack from a malicious program and an attack to try to enter our emails... That happens to us and also to other organizations. (E3 director of HR organization).*

It is significant that organizations located in cities away from the capital, in rural areas, use WhatsApp as the main means of communication and processing of documentation. According to a human rights defender, this generates a greater risk and vulnerability for the organizations.

- *M: The approach to this in the countryside and in the city is different. In the countryside, the use of Internet in general is not so widespread. I'll give you an example, they have a desktop computer and the information is stored there... they don't use the cloud or those types of tools. On phones they only use WhatsApp instead of email, all the information is passed through there... as for social media, they mostly use Facebook and no other... (E3 director of a human rights organization).*

Greater care or protection of the public and private personal accounts of human rights defenders is observed. What is significant is that such care implies a momentary withdrawal and cessation of publications on social media or, in some cases, moderation of their political stance.

- *M: I assumed that my social media became less political... I feel that there is a strong attack when we have to tone down our profiles in order to have peace... it has to do with mental health... as I want to have peace, I have to soften my profile (E1- Defender of Children and Adolescents Rights).*

Another perceived risk is related to digital identity breaches and the lack of data protection laws in the country.

- *M: Nowadays, to request public information they ask you to enter your digital identity and you are totally exposed... this issue affects security and labor protection (E1- Defender of Children and Adolescents Rights).*

A serious incident that illustrates the situation in which civil society organizations find themselves, was the unauthorized recording of a meeting of CSO representatives via Zoom platform as "evidence/accusation" by a Senator to support his position during the discussion of the Law "That establishes the control, transparency and accountability of non-profit organizations".

- *M: We don't have specific cases of espionage... but we have suspicions... for example, the leak of the private meeting we had about the NGO Law, and that was shown during a session in the Senate is something very striking... I do not know what to call it... leak, espionage... but it is very serious (E3 director of the Human Rights Coordinating Committee of Paraguay).*

6. Security strategy

Regarding security strategies, most of the people interviewed refer to measures or strategies they employ in the use of digital tools, such as two-steps verification and security of account passwords, change in the tone of their posts and blocking accounts of aggressors.

- *M: Anonymity is once again a tool because there is a strong persecution and repression... My social media accounts are set to private... I try to make my profile look more casual... so that it does not look so political... two-factor authentication has to be enabled (E1- Defender of Children and Adolescents Rights).*

- *W: I directly block haters... Twitter is the most aggressive... it's like the sewer of everything that happens... I use fingerprint, password... everything... I don't know if I use WhatsApp with two-steps (G1DJ Human Rights Defender, Young, 18 -30).*

Among the organizational measures mentioned is the call, in the form of a campaign, to block accounts and not give visibility to those who promote hate, as well as to start using open-source software.

- *W: Then we started to ask people to report those profiles so that they could be deactivated... A good thing about the platforms is that you can block certain words... I think that adds to the blocking to identify hate through language (G1DJ Human Rights Defender, Young people, 18 -30).*

- *M: We started adopting some measures, for example, we are starting to use LINUX, and using other messaging platforms instead of the conventional ones... as for the information we have in the cloud, we are looking for other ways to protect it better (director of HR organization).*

7. Recommendations from Human Rights defenders

Regarding cybersecurity and HR organizations, defenders recommend:

1. Have a protocol for dealing with and knowing what to do in case of a cyber-attack.
2. Seek creative, simple and accessible formats to disseminate digital rights (podcast, simple images, campaigns, among others).
3. Establish a program or agenda with networks of organizations to make digital violence visible.
4. Articulate among organizations a system of care and protection in cybersecurity.

CONCLUSION

The research conducted on cybersecurity for human rights defenders in Paraguay makes an important contribution to understanding the practices, technological use, risks, and threats related to digital security. One key contribution of the study is the updated mapping of organizations and defenders to establish a baseline for digital security. This will, in turn, enable follow-up and new measurements over time on the issue.

Based on the analysis of both quantitative and qualitative findings, it becomes clear that the level of cybersecurity among organizations and defenders is characterized by a lack of knowledge and fragmentation on the topic of digital security. There is generally little awareness of digital risks or threats, making it difficult for them to comprehend and take action. This lack of training, combined with a growing reliance on digital technologies, reinforces the perception that cybersecurity is unattainable for many without technical expertise.

It is relevant to highlight that the notion of well-being in digital security and digital self-care is deeply influenced by colonized concepts that impose an individual burden on each person to protect themselves. In contexts of inequality, like those faced by defenders in Paraguay, this individualized view is inadequate. As a result, digital security is seen as a privilege, generating frustration and guilt among those who cannot meet the imposed self-care expectations.

The CIRT-PY records statistics of recent cyber incidents reported in the country, especially those occurring in state dependencies. It also reports complaints received from the private sector and the general public. The vulnerabilities identified align with what human rights defenders mentioned, including weak passwords, outdated software, and malware.

Most defenders who participated in the research live and operate in urban areas and value access to and use of technology (feeling it doesn't overwhelm them). However, this access is not always accompanied by the necessary knowledge to ensure effective security. Regarding the use of digital technologies, the majority (63%) operate independently, but a significant number rely on family and friends for assistance. This correlates with qualitative findings that state they had to learn "on the go" during the pandemic and thus could not fully understand the risks involved or make informed decisions about their digital security.

The primary instant messaging service used is WhatsApp (100%), followed by Facebook Messenger (41%) and Telegram (42%). Despite the widespread use of these tools, results show a high percentage of individuals who have never received training in digital security, reaching 76%. This reflects that most human rights defenders lack proper training to identify risks, threats, or safely use technology. Most of the defenders do not conduct digital security risk assessments (91%) and use the same password for all their accounts (56%). Additionally, 94% of respondents indicated that their organization lacks protocols in this area, worsening their vulnerability.

The findings show that digital matters are primarily handled by the communication or IT teams, while smaller organizations assign multiple tasks or roles to the same individuals.

In this context, it becomes crucial to understand that the responses to the security of human rights defenders in Paraguay must have a collective approach. True comprehensive well-being (including digital) can only be achieved by changing the structure so that everyone can enjoy equitable conditions. Cultural and relational transformation is essential to creating an environment where digital security is accessible to all. While the solution is not solely collective, it is also important to remember that self-care remains vital.

The most common types of digital threats typically involve: 1. Unauthorized access (hacking) to email or social media accounts; 2. Phishing: receiving links to fake sites via text messages, instant messaging, or email to steal personal information and access credentials, or install malicious software; 3. Loss of information; 4. Sexual harassment via social media, email, calls, or text messages; 5. Theft of devices (phones, computers, tablets, hard drives, USBs). In recent years, the first two categories have been the most common.

45% of the respondents indicated they had been victims of some form of gender-based violence facilitated by technology, with 40% specifically identifying digital platforms as the medium. The most common types of violence experienced were cyberstalking, discrimination, and sexual harassment on social media, via email, calls, or text messages due to arbitrary reasons related to their gender, sex, or sexual orientation. Some respondents even reported death threats and insults for being women, highlighting the severity of the risks they face.

Moreover, defenders perceive privacy violations and threats to their rights, with many feeling surveilled or monitored. Some individuals reported being listened to through their phones and suspected incidents of espionage and information theft. This context reinforces the importance of not overburdening individuals with the responsibility for their security but instead progressing towards collective and structural solutions.

According to the survey, 78% of those who experienced attacks or threats did not report them, and those who did mentioned reporting them to platforms, the police, or the ombudsman's office. In all cases, they described the process as highly bureaucratic, often reducing the action to a mere formal record of the incidents.

Finally, the security mechanisms adopted by defenders are often instinctive, as the majority reported not having received any training. To protect themselves, they resort to placing their devices on "airplane mode," turning off their phones during meetings, and "toning down their social media profiles."

In conclusion, the research reveals that the notion of well-being in digital security, as we understand it, is deeply colonized, placing the burden of protection on individuals rather than addressing the structural inequalities that perpetuate vulnerabilities. In this context, the digital security of human rights defenders is perceived as a privilege, which creates frustration and guilt for those unable to meet unattainable expectations. It is essential to understand that security responses, particularly for those defending human rights in Paraguay, must adopt a collective approach. Only a profound structural change will achieve comprehensive well-being, including digital security, that is accessible to everyone. This process requires cultural and relational transformation to build a more equitable environment. While self-care remains important, this research emphasizes that the solution is not solely individual, but part of a collaborative and shared strategy to enable everyone to protect themselves and thrive in a more just digital environment.

RECOMMENDATIONS

Based on the data found in the qualitative and quantitative field and the cross-checking with secondary sources, the following points are recommended:

- Priority should be given to awareness-raising and training on digital issues for human rights defenders and organizations. This implies understanding the scope of technological use and the precautions that should be taken to ensure security and enable the development of human rights defense activities.
- Develop simple tools to disseminate basic guidelines for digital security.
- Articulate a platform with organizations dealing with human rights matters to develop protocols for digital security and to respond to different types of cyberattacks.
- Establish a cybersecurity agenda with organizations to anticipate and raise awareness on digital violence cases against human rights defenders and organizations.
- Generate mechanisms to protect human rights defenders and organizations from situations of massive and specific surveillance from all types of sectors (State or criminal groups).
- Involve human rights organizations and defenders in the process of construction and approval of a comprehensive personal data protection law.
- Develop a toolbox with basic and routine digital safety guidelines to follow: use of secure passwords, change them periodically, keep devices updated, use open-source software, implement two-factor authentication to strengthen password security, safeguard the supply chain by reviewing the terms of use, protect stored information, and ideally use encryption technologies.
- Require social media platforms to strengthen their security mechanisms for their use.
- Promote the creation and implementation of digital security protocols by human rights organizations.
- Generate a monitoring practice through the recording of digital violence and violations against human rights defenders and organizations.

BIBLIOGRAPHY

1. Acuña, J. (10 de Octubre de 2017). Hacia una visión de seguridad digital para todos y todas. https://www.tedic.org/hacia-una-vision-de-seguridad-digital-para-todos-y-todas/. Accessed on 9 May, 2024.

2. Aguilar, J. M. (Abril de 2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. Institute of International Studies –University of Chile. Vol.53 №.198 , pages. 169-197. Retrieved from Challenges and opportunities in cybersecurity in Latin America in the global context of cyberthreats to national security and foreign policy. https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-37692021000100169. Accessed on 13 May, 2024.

3. Bewlay, L., Kilbey, H. and Paes, B. (28 October, 2021). Construcción de herramientas digitales en organizaciones de justicia social: Qué considerar antes de empezar. https://www.theengineroom.org/library/building-digital-tools-in-social-justice-organisations-what-to-consider-before-getting-started/. Accessed on 8 July, 2024.

4. Carrillo, E., Sequera, M. Fulchi, L. (2018). La enajenación contínua de nuestros derechos. Sistemas de identidad: biometría y cámaras de vigilancia no regulada. https://www.tedic.org/wp-content/uploads/2018/07/La-enajenaci%C3%B3n-continua-de-nuestros-derechos_TEDIC_2018.pdf. Accessed on 18 June, 2024.

5. Carrillo, E., Bogado, A. and Kostic, B. (2024). Perpetradores de violencia de género en línea. Hoja de ruta para investigaciones. https://www.tedic.org/wp-content/uploads/2024/07/Perpetradores-de-violencia-de-genero-online-1.pdf. Accessed on 10 July, 2024.

6. Cyber Incident Response Center. (2024). Ministerio de Tecnologías de la Información y Comunicación: https://www.cert.gov.py. Accessed on 2 May, 2024.

7. CERT-PY. (2020). Estado de la ciberseguridad en Paraguay. Year 2020. Asunción: Ministerio de Tecnologías de la Información y Comunicación. https://www.cert.gov.py/wp-content/uploads/2022/02/Informe_Ciberseguridad_Paraguay_2020_-_final-2.pdf

8. Report: Estado de la ciberseguridad en el Paraguay. Year 2022. Asunción: CERT-PY/MITIC. https://www.cert.gov.py/wp-content/uploads/2024/01/Informe-Ciberseguridad-Paraguay-2022.pdf. Accessed on 10 May, 2024.

9. Diario ABC Color. (11 November, 2023). Paraguay firma con EEUU acuerdo de ciberseguridad. www.abc.com.py/politica/2023/11/11/paraguay-firma-con-eeuu-acuerdo-de-ciberseguridad/. Accessed on 26 May, 2024.

10. Diario La Nación. (6 July, 2023). Destacan hito en ciberseguridad paraguaya tras acuerdo de cooperación con EE. UU. www.lanacion.com.py/politica/2023/07/06/destacan-hito-en-ciberseguridad-paraguaya-tras-acuerdo-de-cooperacion-con-ee-uu/. Accessed on 13 June, 2024.

11. Diario Última Hora. (6 de Enero de 2024). Obtenido de MITIC no desconoce incidente de ciberseguridad de telefonía: www.ultimahora.com/mitic-no-desconoce-incidente-de-ciberseguridad-de-telefonia. Accessed on 9 May, 2024.

12. Fundación Karisma. (2024). Consideraciones para un plan de respuestas a incidentes de ciberseguridad. Obtenido de Bogotá: https://web.karisma.org.co/consideraciones-parael-diseno-de-un-plan-derespuesta-a-incidentesde-ciberseguridad/. Accessed on 23 July, 2023.

13. Fundación Karisma. (2024). Comentarios al borrador del decreto de ciberseguridad del MinTIC. https://web.karisma.org.co/comentarios-al-borrador-del-decreto-de-ciberseguridad-del-mintic/. Accessed on 25 July, 2024.

14. Machín, N. y. (October, 2016). Ciberseguridad como factor crítico en la seguridad de la Unión Europea. Madrid: Universidad Compluetense. Magazine UNISCI. № 42. pp. 47-68: https://www.redalyc.org/pdf/767/76747805002.pdf. Accessed on 15 May, 2024.

15. Martínez, E. y. (April, 2021). Revista digital de Ciencia, Tecnología e Innovación. ISSN 1390-9150. Vol. 8. №2. pp. 221-234. Retrieved from Cybersecurity in social networks: a theoretical review.

16. Public Prosecutor's Office. (2024). Unidad Especializada de Delitos Informáticos. https://ministeriopublico.gov.py/unidad-especializada-de-delitos-informaticos-. Accessed on 6 May,2024.

17. Ministry of Technology, Information and Communication. (6 June, 2024). Por qué es importante para el Paraguay actualizar su Estrategia Nacional de Ciberseguridad. https://mitic.gov.py/por-que-es-importante-para-el-paraguay-actualizar-su-estrategia-nacional-de-ciberseguridad/. Accessed on 12 June, 2024.

18. United Nations. (1998). La Declaración de los defensores de los derechos humanos. Resolución A/RES/53/144. Retrieved from Office of the High Commissioner of Human Rights. https://www.ohchr.org/es/special-procedures/sr-human-rights-defenders/declaration-human-rights-defenders. Accessed on 8 June, 2024.

19. United Nations. (2011). Offices of the High Commissioner for Human Rights: Colombia, Guatemala and México. Comentarios sobre la declaración de defensores y defensoras de derechos humanos. https://www.corteidh.or.cr/tablas/28995.pdf. Accessed on 16 May, 2024.

20. United Nations. (2024). Acerca de los defensores de los derechos humanos. Relator Especial sobre los defensores de los derechos humanos. Retrieved from Office of the High Commissioner of Human Rights. https://www.ohchr.org/es/special-procedures/sr-human-rights-defenders/about-human-rights-defenders#:~:text=Los%20defensores%20act%C3%BAan%20en%20favor,-circulaci%C3%B3n%20y%20la%20no%20discriminaci%C3%B3n. Accessed on 13 May, 2024.

21. OECD. 2016. Políticas de banda ancha para América Latina y el Caribe: Un manual para la economía digital. Gestión de riesgos de seguridad. Obatined from: digitalhttps://read.oecd-ilibrary.org/science-and-technology/politicas-de-banda-ancha-para-america-latina-y-el-caribe/gestion-de-riesgos-de-seguridad-digital_9789264259027-17-es#page3. Accessed on 20 June, 2024.

22. Organization of American States. (8 June, 2004). Resolution AG/RES. 2004 (XXXIV-O/04) "Adopción de una estrategia interamericana integral para combatir las amenazas a la seguridad cibernética: un enfoque multidimensionales y multidisciplinario para la creación de una cultura de seguridad cibernética". Obtained from https://www.oas.org/en/citel/infocitel/julio-04/ult-ciberseguridad_e.asp. Accessed on 18 May, 2024.

23. United Nations Human Rights Office. (2019). Derechos a la libertad de reunión pacífica y de asociación. https://www.ohchr.org/. Accessed on 4 June, 2024.

24. Paes, B. (28 June, 2024). Un ejercicio de imaginación: el trabajo de fortalecer los ecosistemas de información. https://www.theengineroom.org/library/an-exercise-in-imagination-the-work-of-strengthening-information-ecosystems/. Accessed on 15 July, 2024.

25. Ramírez, A. (23 December, 2023). Ciberdefensa como estrategia para seguridad y soberanía digital en Paraguay. Retrieved from Revista Jurídica: Investigación en Ciencias Jurídicas y Sociales. № 14.1. Págs 16-41: https://ojs.ministeriopublico.gov.py/index.php/rjmp/article/view/327. Accessed on 19 May, 2024.

26. Foco Magazine. (30 November, 2018). 4 Pautas para proteger la seguridad digital de tu emprendimiento. Obtained from https://foco.lanacion.com.py/2018/11/30/4-pautas-para-proteger-la-seguridad-digital-de-tu-emprendimiento/. Accessed on 16 May, 2024.

27. Sancho Hirare, C. (2017). Ciberseguridad. Presentación del dossier. Obtained from URVIO, Latin American Journal of Security Studies, № 20, pp. 8-15: https://www.redalyc.org/journal/5526/552656641001/html/. Accessed on 17 May, 2024.

28. Sequera, M. (2022). Manifestaciones libres. Guía sobre la vigilancia policial en manifestaciones en Paraguay. https://www.tedic.org/wp-content/uploads/2022/03/Guia-Manifestaciones-libres-WEB.pdf. Accessed on 12 June, 2024.

29. Sequera, M. and Acuña, J. (2023). La violencia digital de género a periodistas en Paraguay. https://www.tedic.org/wp-content/uploads/2023/10/Violencia-Genero-Periodistas-TEDIC-2023-web-2.pdf. Accessed on 18 May, 2024.

30. Sequera, M. and Samaniego, M. (2018). Cibercrimen: desafíos de la armonización del Convenio de Budapest en el sistema penal paraguayo. https://www.tedic.org/wp-content/uploads/2018/10/minuta_TEDIC.pdf. Accessed on 3 June, 2024.

31. Sequera, M., Toledo, A. and Ucciferri, L. (2018). Derechos Humanos y Seguridad Digital: una pareja perfecta. Aportes de la sociedad civil hacia políticas nacionales de seguridad digital que respeten y protejan los derechos humanos. https://www.tedic.org/wp-content/uploads/2018/12/InformeCiberseguridadParte1.pdf. Accessed on 8 July, 2024.

32. Sequera, M. and Rolón Luna, J. (2016). Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Paraguay. TEDIC y Electronic Frontier Foundation. https://www.tedic.org/wp-content/uploads/2018/12/Vigilancia-estatal-de-las-comunicaciones-y-derechos-fundamentales-en-Paraguay.pdf. Accessed on 5 July, 2024.

33. Sequera, M. (2019). El billetaje electrónico. Nuestros derechos están en juego. Obtained from www.tedic.org/el-billetaje-electronico-nuestros-derechos-estan-en-juego

34. Paraguay Legislative Information System. Bill. #Expediente: D-2164736. https://silpy.congreso.gov.py/web/expediente/124598. Accessed on 6 July, 2024.

35. TEDIC. (June 2016). Comentarios al Borrador del Plan Nacional de Ciberseguridad. Obtained from https://www.tedic.org/wp-content/uploads/2016/06/observaciones-sobre-el-plan-de-ciberseguridad_v14jun-.pdf. Accessed on 1 June, 2024.

36. TEDIC. (8 March, 2018). Obtenido de Derechos humanos y seguridad digital: una pareja perfecta. https://www.tedic.org/derechos-humanos-y-seguridad-digital-una-pareja-perfecta/. Accessed on 13 May, 2024.

37. TEDIC. (2 October, 2018). Hacia una justicia penal que hable el lenguaje de Internet. Obtained from https://www.tedic.org/hacia-una-justicia-penal-que-hable-el-lenguaje-de-internet/. Accessed on 23 May, 2024.

38. LAWS, DECREES AND REGULATIONS CONSULTED

39. Decree № 11.624/2013, "Whereby Law № 4989 of August 9, 2013, is regulated and creates the framework for the application of Information and Communication Technologies in the public sector and creates the National Secretariat of Information and Communication Technologies (SENATICs) and establishes the organizational and functional structure of the aforementioned National Secretariat".

40. Decree № 5323/2016, "Whereby Arts. 20 and 21 of Law № 4989/2013": "Which creates the framework for the application of ICTs in the public sector and creates the National Secretariat of Information and Communication Technologies (SENATICs)".

41. Decree № 8098/2022, regulation of law 5653/2016: "On the protection of children and adolescents against harmful internet content".

42. Decree № 2274/2019, regulation of Law № 6.207/2018: "Which creates the Ministry of Information and Communication Technologies and establishes its organic charter".

43. Decree № 6234/2016, "Whereby the application and use of information and communication technologies (ICT) is declared of national interest, the minimum structure it must have is defined and other provisions are established for its effective operation".

44. Decree № 7052/2017, "Whereby the National Cybersecurity Plan is approved and the National Cybersecurity Commission is integrated".

45. Decree № 7576 /2022, regulation of Law No. 6822/2021: "On trust services for electronic transactions, electronic transferable documents".

46. Law № 4989/2013, “Which creates the framework for the application of information and communication technologies in the public sector and creates the National Secretariat of Technologies, Information and Communication (SENATICs)”.

47. Law № 6822/2021, “On trust services for electronic transactions, electronic documents and electronic transferable documents”.

48. Law № 5653/2016, “On the protection of children and adolescents against harmful internet content”.

49. Law № 6.207/2018, “Which creates the Ministry of Technologies, Information and Communication and establishes its organizational charter”.

50. Resolution MITIC N° 699/2019, Approval of the “Minimum Security Criteria for the Development and Acquisition of Software”.

51. Resolution MITIC № 346/2020, “Whereby the regulations for mandatory reporting of cyber security incidents by the State Agencies and Entities (OEE) to the Ministry of Information and Communication Technologies (MITIC), through the Cyber Incident Response Center (CERT-PY) are approved and implemented”.


Technology
& Human
Rights