https://doi.org/10.55738/journal.v11i2p.86-98

Digital Security in Youth: The Salvadoran Case

Seguridad digital en jóvenes: el caso salvadoreño

Segurança digital nos jovens: o caso salvadorenho

Karla Patricia Ramos Amaya, Ph.D.
Universidad Centroamericana José Simeón Cañas
El Salvador
kpramos@uca.edu.sv

Abstract: This manuscript provides a detailed account of the original findings from a research project on digital security in Salvadoran youth conducted in 2021 and published in 2022. This work falls within the action framework of the Media and Information Literacy Program "Alfabeta Media Lab," involving two Salvadoran universities. The research aims to understand the digital security practices and tools used by Salvadoran youth aged 16 to 24, identifying shortcomings that can inform future support and solutions. The methodology adopts a quantitative-qualitative approach, employing a questionnaire with a representative sample of 976 young individuals from both rural and urban areas across 13 of the 14 departments of the country, along with three focus groups consisting of 28 participants in total. The study's results underscore the importance of fostering digital security competencies within Media and Information Literacy to enhance critical thinking and responsible, active citizenship, promoting an ethical and contextually relevant approach to media products. Within this framework, digital security transcends mere technological instrumentality and becomes a practice with social consciousness.

Keywords:
Digital Security, Media and Information Literacy, Youth Salvadoran, Digital Competence, Media Literacy, Digital Literacy

Resumen: Este manuscrito presenta, de manera detallada, los resultados originales del proyecto de investigación sobre Seguridad Digital en jóvenes Salvadoreños realizado en 2021 y publicado en 2022. Este trabajo se enmarca dentro de los ejes de acción del Programa de Alfabetización

Mediática e Informacional “Alfabeta Media Lab”, del que participan dos universidades salvadoreñas. Esta investigación pretende conocer las prácticas y herramientas sobre seguridad digital presentes en los jóvenes salvadoreños de 16 a 24 años para identificar falencias que permitan en un futuro elaborar propuestas de apoyo y solución a las mismas. La metodología asume una perspectiva cuantitativa-cualitativa. Se aplicó un cuestionario con muestra representativa de 976 jóvenes del área rural y urbana en 13 de los 14 departamentos del país y se desarrollaron 3 grupos focales con 28 jóvenes en total. Los resultados de este estudio reafirman la importancia de formar competencias sobre seguridad digital en clave de Alfabetización Mediática e Informacional para fortalecer el pensamiento crítico y la ciudadanía activa responsable, lo cual implica acercarse a los productos mediáticos con una visión ética y cercana al contexto. Dentro de este marco, la seguridad digital es más que una instrumentalización de las tecnologías y se convierte en una práctica con conciencia social.

Palabras clave:
Seguridad Digital, Alfabetización Mediática e Informacional, Jóvenes salvadoreños, Competencia Digital, Alfabetización Mediática, Alfabetización Digital

Resumo: Este manuscrito apresenta, detalhadamente, os resultados originais do projeto de pesquisa sobre Segurança Digital em jovens salvadorenhos realizado em 2021 e publicado em 2022. Este trabalho enquadra-se nos eixos de ação do Programa de Alfabetização Midiática e Informacional “Alphabeta Media Lab”, do qual participam duas universidades salvadorenhas. Esta pesquisa visa compreender as práticas e ferramentas de segurança digital presentes nos jovens salvadorenhos entre 16 e 24 anos para identificar deficiências que permitirão no futuro desenvolver propostas de apoio e soluções para elas. A metodologia assume uma perspectiva quanti-qualitativa. Foi aplicado um questionário a uma amostra representativa de 976 jovens de áreas rurais e urbanas em 13 dos 14 departamentos do país e foram desenvolvidos 3 grupos focais com 28 jovens no total. Os resultados deste estudo reafirmam a importância da formação de competências em segurança digital em termos de Literacia Mediática e Informacional para fortalecer o pensamento crítico e a cidadania ativa responsável, o que implica abordar os produtos mediáticos com uma visão ética próxima do contexto. Neste quadro, a segurança digital

é mais do que uma instrumentalização de tecnologias e torna-se uma prática socialmente consciente.

Palavras-chave:
Segurança digital, Alfabetização Midiática e Informacional, Juventude salvadorenho, Competência digital, Alfabetização Midiática, Alfabetização digital

1. Introduction

Digital security is an increasingly exciting topic studied from various perspectives. According to UNESCO (2011), digital security is part of the skills and knowledge included in Media and Information Literacy, which is essential for developing critical thinking and effective interaction with messages and media (UNESCO, 2011). This practical interaction highlights a broad general and conceptual framework, which, from the perspective of Ferrés and Piscitelli (2012) and Durán-Becerra and Lau (2020), should articulate other more specific dimensions for its development, such as the following:

1. Informational: the ability to access, evaluate, and critically understand information (Durán-Becerra & Lau, 2020, pp. 58-59).
2. Digital: related to the basic and advanced use of ICT. This includes, among other aspects, the design of solutions and strategic and reflective decision-making with ICT (Durán-Becerra & Lau, 2020, p. 60).
3. Media: dealing with a complex phenomenon by combining participatory culture with developing critical capacity (Ferrés & Piscitelli, 2012, p. 77). That is, the development of skills and abilities to understand the meaning, operation, and context of media; participation in networks, online government, making security decisions, sharing knowledge, and understanding the ethical and legal aspects of media use (Durán-Becerra & Lau, 2020, pp. 60-61).

This last dimension is one of the most related to digital security, which acquires a meaning of protection against problems generated by the use of ICT (Barrow and Heywood-Everett, 2006, as cited in Gallego-Arrufat et al., 2019) and is related to privacy, integrity, and also promoting, modeling, and training digitally responsible citizens, to counteract or minimize risks of social engineering known as the science and art of deceiving humans, which is

increasing, according to the Data Breach Investigations Report (Verizon, 2018, as cited in Conde, 2021). Some examples where it manifests are phishing (identity impersonation through fake emails), smishing (fraud executed through messages to encourage clicks on malicious sites), malware or software that pretends to be legitimate, pretexting (the practice of presenting oneself as another person to obtain private information (Susatama Hurtado, 2022) among others.

In Central America, some studies have shown an increase in interest and relevance of this topic to generate recommendations or guidance on public policies. One of the first examples is the research conducted by Castillejos et al. (2016), who investigated the topic of security in the digital competencies of millennials in Mexico. The study pointed out that many students were cautious when receiving unknown messages. The study also revealed habits such as blocking pages of dubious origin, periodically changing passwords, and using "green" technologies as an innovative contribution.

In Costa Rica, the Central American Observatory of Digital Security of the Fundación Acceso (2019) researched privacy and digital surveillance in El Salvador. It recommended that people linked to human rights be trained to generate synergies so that entities and individuals have better digital security.

In the same line, the Asociación Comunicares (2021) presented the results of the study "Desde nuestra mirada," in which it was found that 28% of young people used the same password in all their networks. At the same time, 54% opened a new Facebook account because they forgot their original password. Only 9% use passwords combining four types of characters: uppercase, lowercase, numbers, and symbols.

Although these studies provide some indications in the region, more data from primary sources are still needed. It is essential to inquire about the subject, particularly in El Salvador, considering that Salvadoran youth represent 54.1% of the population, according to the Dirección General de Estadística y Censos (2020).

This article represents research focused on Salvadoran youth aged 16 to 24 from rural and urban areas in El Salvador. Although this is an initial approach, it aims to:

a) Learn about the various practices and tools of digital protection used by young people.

b) Generate data to develop inputs for future action plans.

The study seeks to understand in more detail the local situation in terms of digital security, responding to the following question: What practices and beliefs about digital security can be observed among Salvadoran youth aged 16 to 24 in urban and rural areas?

2. Methodology/approach

A mixed method was used. Morse (2003) notes that one of its main advantages is allowing the development of a broader and more comprehensive study. Tashakkori and Teddli (1988) propose a mixed-design taxonomy of equivalent status. The study used qualitative and quantitative approaches to answer research questions. Data were collected simultaneously and analyzed complementarily.

For data collection, a quantitative online questionnaire with closed responses was used. Due to the difficulty of ensuring randomness in selecting individuals, a non-probabilistic sampling was used. The qualitative data collection strategy was implemented by implementing three focus groups in three main areas of El Salvador.

Subsequently, the data were analyzed, which, according to Hernández-Sampieri and Mendoza (2020), should follow the procedures of each approach. In the case of the quantitative, basic descriptive and inferential statistics were used, and the qualitative through category coding. Thus, for the quantitative, the data were dumped into an Excel matrix, and then each question was visualized to later triangulate it with what was found within the qualitative categories. The categories of analysis were defined based on the question and research objectives and are described below: connection devices, passwords, public data, and trust in the web.

Regarding the number of participants, the purposive or judgmental choice does not start from a predetermined number, as defined by Patton (2001), "in this field, there are no rules to say the size of the sample, and if there had to be one, it would be it all depends" (p. 224). Based on the above, a sample of the Salvadoran population over 16 years old (asked for consent signed by their legal guardians) and those under 25 (also asked for permission to be part of this study) was used.

A questionnaire was applied to 976 young people in 37 public and private educational centers in rural and urban areas. And in the focus groups, 28 young people from three different regions of the country participated.

3. Results

By geographic distribution, there were young people from 13 of the 14 departments of El Salvador: 29.9% from San Salvador, 21.6% from Santa Ana, 13.7% from San Miguel, and 3.5% from La Libertad. This distribution included rural and urban areas.

Following the objectives set, data were generated to learn about young people's practices and tools of digital protection. The details of these will be grouped into the categories previously established.

3.1 Devices and connection

With or without the internet, the cell phone (96.3%), the laptop (64.8%), and the tablet (12.1%) are the most used technologies. Regarding connection time, 70% stay online for more than three hours. The majority reported using residential internet, followed by prepaid and postpaid modalities. Connections in study centers, parks or public places, and cyber cafes were also recorded by young people, less frequently, as a point of access to the network.

3.2 Passwords

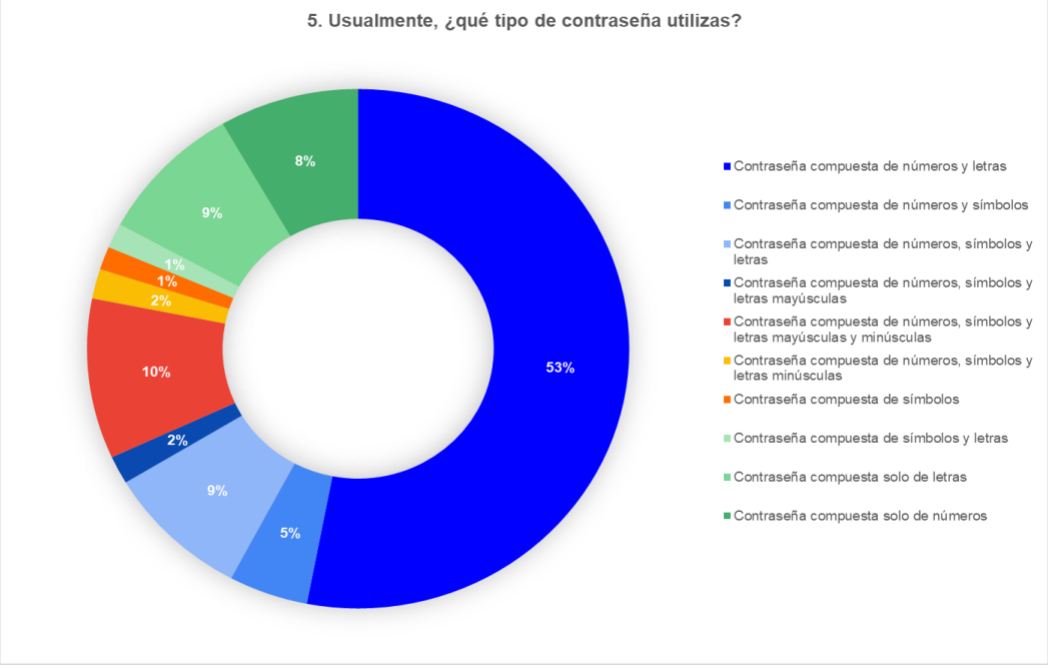

Figure 1. Type of password. Source: Own elaboration.

More than 61% of young people use insecure passwords. When they forget them, six out of ten young people reset them by email, 9% through two-step verification, and the rest (23%) do it through a phone number.

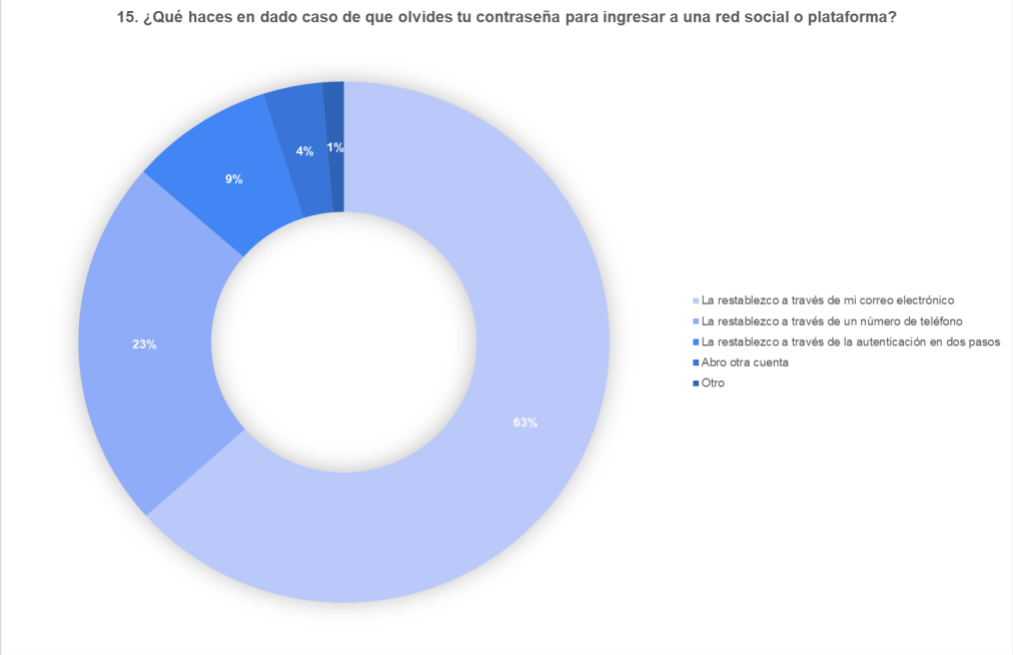

Figure 2. Account recovery. Source: Own elaboration.

The respondents' response leaves aside two-step authentication, through which banking sites, social networks, video games, and email platforms must verify a person's identity in different ways, ensuring two of them (Marchal, 2019). These can be through a code, fingerprint, or previously saved personal questions. Main servers like Google, Apple, or Outlook recommend its implementation to reinforce web services.

84.9% do not know any application designed for password management. This lack of knowledge represents an opportunity for training for educational institutions so that they can delve into these cybersecurity tools.

Only 31% of young people use a different password for each account they have created. To this is added another element, and that is that 40% never update them. Those who do are divided among the following percentages: 26% every six months and 10.0% quarterly.

Although 70.0% of young people said they do not share their passwords, focus groups showed this is not so real. Young people know it is not advisable to share it; however, many share it with parents, friends, and sentimental partners, in that order.

This sharing adds to the fact that more than half (53.5%) indicated that they have also shared their electronic devices with family and close friends; only four out of ten do not do it.

3.3. Published data

Figure 3. Type of information published. Source: Own elaboration.

Most prefer to publish their name (42%), place of residence (35%), and where they study (35%). The telephone number and workplace (3.4%) appear least on their networks. The young respondents post accurate information depending on their situation and platform. Two out of ten stated they never post accurate data. Added to this are mentions of friends or relatives and, according to the findings, four out of ten tag their contacts and publish their actual location.

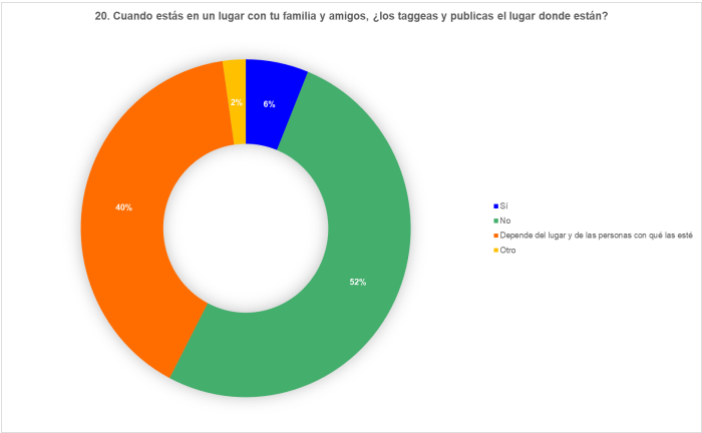

Figure 4. Tags to close contacts. Source: Own elaboration.

When talking with the young people about posting data in real-time, several mentioned that they wait to get home for safety reasons. As for the information they back up, five out of ten do not do it, nor do they know there are applications for this. The rest state that they do.

3.4 Trust in the Web

They must disagree with the belief that the government controls their private information and personal data. They also do not believe that the phone and messaging apps spy on or are interested in their conversations. This apathy in spying is an element that attracts attention because the "appropriation" of citizens' data has been increasing over time (Ricoy Casas, 2018), and violations are daily.

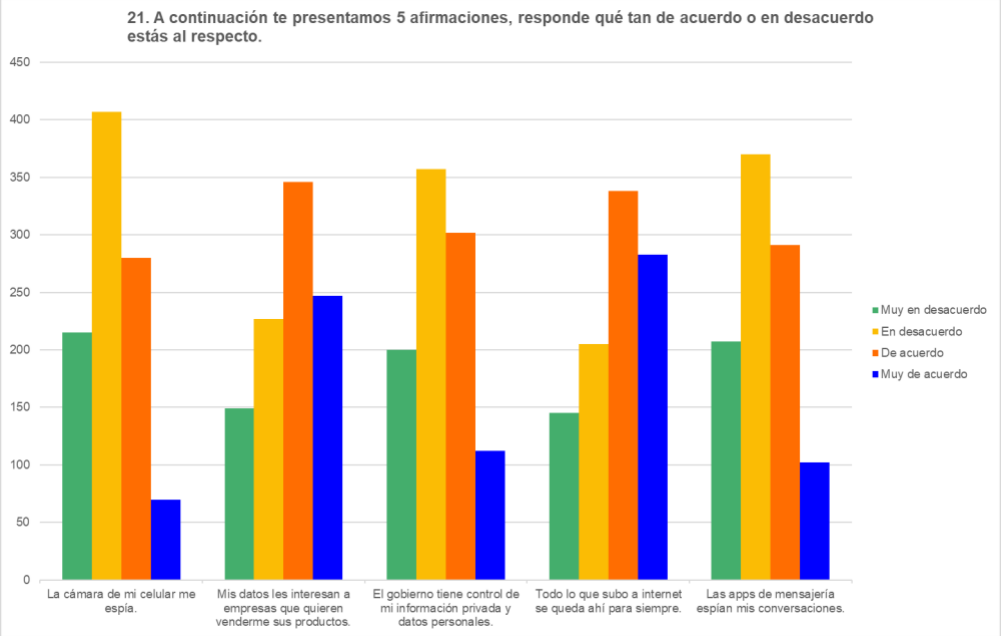

Figure 5. Statements about trust in the web. Source: Own elaboration.

On the other hand, they most agree that their data is of interest to companies that want to sell them products and that everything uploaded to the network remains there.

4. Discussion of Results

4.1 Children of Their Time

Salvadoran youth remain connected to the internet with an electronic device 99% of the time, a high percentage very characteristic of the 21st-century culture, in which technology is used to replace stability and borders with movement, experience with post-experience, effort

with fun, depth with superficiality, and collectivity with mass individualism (Baricco, 2008). We live in a world whose limits with the physical world have been fading, reaching a point where our transition from one to the other is constant and increasingly less perceptible.

4.2 Practices with Manifest Deficiencies

Most young people use passwords with low levels of protection, i.e., 53.0% prefer them only with numbers and letters. Moreover, they log in with the same ones to their different accounts. With this practice, they are ignoring the recommendations made by competent entities, who recommend including special characters and symbols and differentiating the "passwords" in emails, apps, and bank accounts. This finding highlights a deficiency in the digital dimension since there is little understanding of the media's meaning, operation, and context in making security decisions (Ferrés & Piscitelli, 2012).

4.3 Informational Dimension Partially Present

The results showed that informational competence (Durán-Becerra & Lau, 2020) is partially applied. Young people have enough technical skills to access, evaluate, and understand aspects of device operation, but with the absence of many other criteria. This aspect becomes relevant in a digital environment where young people are aware of fraud and identity theft cases such as phishing, malware, pretexting, and smishing, which, according to Susatama Hurtado (2022), are the most common within social engineering.

4.4 Violence on the Network and Cyberattacks

Violence is a transversal axis present in relationships mediated by the internet. The results showed that a considerable group waited to reach a safe place to publish their location and indicate the people they were with. Some respondents mentioned cases of bullying, identity theft, hacking, grooming, and others.

4.5 The School, an Indispensable Actor

Most young people stated that they learned about cybersecurity through tasks or activities within educational centers. Thus, the role of the school as a thought-building agent among its students is reaffirmed.

5. Conclusions

Digital security regarding Media and Information Literacy points to the development of critical thinking and responsible, active citizenship. It is oriented more than to the instrumentalization of technologies to practice with awareness against the various attacks of social engineering.

Another conclusion is that there is a need to think about digital security in terms of Media and Information Literacy to question, distance, and renounce the importance of emotions in audiences' consumption habits to safeguard users' integrity. In light of the results, this remains a pending issue that must continue to be addressed with full awareness of the complexity of the context. Finally, the study highlighted the need to educate in understanding messages, advertising, sources, and interests to which these respond. They can also use media and information literacy, which is necessary for democracy and justice. This use of media and information creates emancipated spectators, as Rancière (2010) said, in favor of liberating education, or, as the teacher Freire (1968) taught, teaching that investigates because there is no teaching without research nor research without instruction. We all know something and are ignorant of something; that's why we always learn.

6. References

Asociación Comunicares. (2021). *Presentación de resultados: Desde Nuestra Mirada* [Diapositivas]. https://comunicares.com/archivo/presentacion-ejecutiva-exposicion-de-resultados-desde-nuestra-mirada

Baricco, A. (2008). *Los bárbaros: ensayo sobre la mutación.* Anagrama.

Castillejos López, B., Torres Gastelú, C. A., & Lagunes Domínguez, A. (2016). La seguridad en las competencias digitales de los millennials. *Apertura*, 8 (2), 54-69. https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1665-61802016000300054

Conde, J. (2021). Concientización en Ciberseguridad a través de Ataques de Ingeniería Social. *INF-FCPN-PGI Revista PGI*, (7), 62–64. https://ojs.umsa.bo/ojs/index.php/inf_fcpn_pgi/article/view/109

Dirección General de Estadística y Censos (DIGESTYC). (2020). Encuesta de Hogares de Propósitos Múltiples 2019. https://www.transparencia.gob.sv/institutions/minec/documents/401354/download

Durán-Becerra, T., & Lau, J. (2020). MIL Competency Framework: Mapping Media and Information Competencies. *Anagramas -Rumbos y sentidos de la comunicación-*, 19 (37), 49-67. https://doi.org/10.22395/angr.v19n37a3

Ferrés, J., y Piscitelli, A. (2012). La competencia mediática: propuesta articulada de dimensiones e indicadores. *Revista Comunicar*, 19 (38), 75-82. https://doi.org/10.3916/C38-2012-02-08

Freire, P. (1968). *Investigación y metodología de la investigación del tema generado*. ICA.

Fundación Acceso. (2019). Observatorio Centroamericano de Seguridad Digital. https://www.acceso.or.cr/wp-content/uploads/2021/08/2019-OSD.pdf

Gallego-Arrufat, M. J., Torres-Hernández, N., y Pessoa, T. (2019). Competencia de futuros docentes en el área de seguridad digital. *Comunicar: Revista científica de comunicación y educación*, 27 (61), 57-67. https://doi.org/10.3916/C61-2019-05

Hernández-Sampieri, R., & Mendoza, C. (2020). *Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta*. McGraw-Hill.

Marchal, D. (2019). PSD2: Pagos más seguros a partir de ahora. *Red seguridad: revista especializada en seguridad de la información*, 86, 52-54. https://www.redseguridad.com/revistas/red/086/52/index.html#zoom=z

Morse, J. M. (2003). Principles of mixed methods and multimethod research design. In A. Tashakkori & C. Teddlie (Hrsg.), *Handbook of mixed methods in social and behavioral research* (pp. 189–208).

Patton, M. Q. (2001). *Qualitative research and evaluation and methods* (3a. ed.). Sage.

Rancière, J. (2010). *El espectador emancipado.* Bordes Manantial.

Ricoy Casas, R. M. (2018). Algunos ejemplos de espionaje y vulneración de la protección de datos a escala mundial. *Revista de la Escuela Jacobea de Posgrado*, 14, 51-68. https://www.jacobea.edu.mx/revista/numeros/numero14/3.-Rosa-Ricoy-Casas-Ejemplos-Espionaje-Vulneracion.pdf

Susatama Hurtado, M. A. (2022). *Análisis de las técnicas más usadas en la ingeniería social*. Universidad Piloto de Colombia. http://repository.unipiloto.edu.co/handle/20.500.12277/12497

Tashakkori, A., & Teddlie, C. (1998). *Mixed methodology: Combining qualitative and quantitative approaches*. Sage.

UNESCO. (2011). Alfabetización Mediática e Informacional: Curriculum para Profesores. *UNESCO*. https://unesdoc.unesco.org/ark:/48223/pf0000216099