Revista Iberoamericana para la Investigación y el Desarrollo Educativo
ISSN 2007 - 7467

https://doi.org/10.23913/ride.v15i29.2098

Artículos científicos

Ciberviolencia perpetrada por estudiantes de secundaria a docentes de Sinaloa, México: percepción, incidencia y estrategias de afrontamiento

Cyberviolence perpetrated by secondary school students Against Teachers in Sinaloa, Mexico: Perception, Incidence, and Coping Strategies

Violência cibernética perpetrada por estudantes do ensino médio contra professores em Sinaloa, México: percepção, incidência e estratégias de enfrentamento

María Luisa Pereira Hernández
Universidad Pedagógica del Estado de Sinaloa, México
pereirahdz@hotmail.com
https://orcid.org/0000-0002-4748-5397

Resumen

El estudio se enfoca en analizar la incidencia y las características de la ciberviolencia hacia los docentes en el estado de Sinaloa, México. Se empleó una metodología cuantitativa de alcance exploratorio descriptivo para obtener una comprensión integral del fenómeno. Se aplicó una encuesta validada por jueces de 33 preguntas a 852 docentes de secundarias estatales, del Estado de Sinaloa. Los resultados revelaron ciberataques y ciberbullying hacia los docentes, el 77% informó conocer a compañeros y el 16.9% compañeras víctimas, se identificaron diversas estrategias de afrontamiento utilizadas por los afectados, incluyendo el diálogo con el estudiantado (45) y la comunicación con las autoridades escolares (22). Los hallazgos destacan la necesidad de una mayor conciencia y capacitación sobre ciberseguridad en el ámbito educativo, así como de políticas efectivas para abordar el ciberbullying. Las conclusiones principales subrayan la importancia de promover una cultura de seguridad cibernética en las escuelas y de implementar intervenciones específicas para prevenir y mitigar la ciberviolencia del estudiantado al docente.

Palabras clave: ciberbullying, ciberacoso, formación de docentes, ciberseguridad, tecnología educativa.

Abstract

The study focuses on analyzing the incidence and characteristics of cyberviolence towards teachers in the state of Sinaloa, Mexico. A quantitative methodology with an exploratory descriptive scope was used to obtain a comprehensive understanding of the phenomenon. A 33-question survey, validated by experts, was applied to 852 secondary school teachers in Sinaloa. The results revealed cyberattacks and cyberbullying towards teachers, with 77% reporting knowing colleagues who were victims and 16.9% reporting knowing female colleagues who were victims. Various coping strategies used by the affected teachers were identified, including dialogue with students (45) and communication with school authorities (22). The findings highlight the need for greater awareness and training on cybersecurity in the educational field, as well as effective policies to address cyberbullying. The main conclusions emphasize the importance of promoting a culture of cybersecurity in schools and implementing specific interventions to prevent and mitigate student-to-teacher cyberviolence.

Keywords: cyberbullying, cyberharassment, teacher training, cybersecurity, technology education.

Resumo

O estudo se concentra em analisar a incidência e as características da ciberviolência contra professores no estado de Sinaloa, México. Utilizou-se uma metodologia quantitativa de escopo exploratório descritivo para obter uma compreensão abrangente do fenômeno. Uma pesquisa validada por juízes com 33 perguntas foi aplicada a 852 professores do ensino médio estadual do Estado de Sinaloa. Os resultados revelaram ataques cibernéticos e cyberbullying contra professores, 77% relataram conhecer colegas de classe e 16,9% outras vítimas, foram identificadas várias estratégias de enfrentamento utilizadas pelas pessoas afetadas, incluindo o diálogo com os alunos (45) e a comunicação com as autoridades (22). As conclusões destacam a necessidade de uma maior sensibilização e formação em segurança cibernética na educação, bem como de políticas eficazes para combater o cyberbullying. As principais conclusões destacam a importância de promover uma cultura de cibersegurança nas escolas

e de implementar intervenções específicas para prevenir e mitigar a ciberviolência dos alunos aos professores.

Palavras-chave: cyberbullying, cyberbullying, formação de professores, cibersegurança, tecnologia educacional.

Fecha Recepción: Abril 2024 **Fecha Aceptación:** Septiembre 2024

Introduction

The growing penetration of digital technology in everyday life has introduced a series of challenges and threats, among which the phenomenon of cyberattacks stands out. In Mexico, as in many other countries, cyberbullying represents an increasingly pressing concern, with significant repercussions for the security and well-being of the population, especially among young people and women. In this context, teachers have not been immune to these forms of digital violence, facing cyberattacks perpetrated by students, parents, and colleagues (Challenor, 2019; De Wet, 2010; González, 2024; Huang et al., 2014; Kauppi and Pörhölä, 2012a; Kauppi and Pörhölä, 2012b; Kopecký and Szotkowski, 2017; Mooij, 2011; Pereira, 2021; Pereira, 2023; Pereira, 2024; Tolentino, 2016). However, the lack of data and the low reporting rates have made it difficult to fully understand this phenomenon and to implement adequate prevention and protection measures. In this regard, there is a need to investigate the data related to the cyberattacks faced by teachers in the state of Sinaloa in order to better understand the nature and magnitude of this problem, as well as to design effective intervention strategies.

In 2019, more than 25% of Mexicans aged 12 to 19 were victims of cyberbullying. This phenomenon particularly affects women in this age group, with 28% experiencing various forms of cyberbullying, including calls, messages, multimedia content, identity theft, and the publication of personal information. An alarming fact is that 80% of victims stated they did not know the identity of their harassers, which underscores the complexity and anonymity that characterize cyberbullying in the digital age. This increase in cyberbullying cases highlights the urgent need to address this problem and implement effective measures to protect young people online (Instituto del Derecho de las Telecomunicaciones [IDET], 2020).

During the first nine months of 2020, Mexico was the most attacked country in Latin America, accounting for more than 22% of ransomware attacks in the region and affecting

nearly 300,000 companies. Additionally, a significant number of Mexicans were victims of cybercrime in 2017, resulting in an economic impact of billions of dollars (IDET, 2020).

The increase in cybercrime has significantly impacted Mexico, especially with a notable rise in attacks on critical infrastructure, fraud, identity theft, and ransomware. Between September and October 2020, more than 10,000 cyberattacks were recorded. This rise is attributed to the rapid adoption of new technologies, such as artificial intelligence and big data, which have enhanced the capabilities of cyber attackers, affecting both citizens and public and private institutions. The economic and social repercussions are evident, with Mexican companies facing million-dollar losses due to ransomware attacks and an alarming increase in cybercrime victimization, particularly among young people. This situation makes it imperative to rethink national security and cybersecurity strategies in the context of accelerated digital transformation (IDET, 2020).

There is alarming data regarding the cybersecurity landscape in Mexico. In 2021, Mexico experienced 156 billion cyberattack threats, with cyber fraud amounting to eight billion dollars annually. Additionally, a 600% increase in cyberattack attempts in Latin America and the Caribbean was reported for the same year (IDET, 2022).)

In the current cyber threat landscape, a significant increase of 28% in cyberattacks was recorded in 2022 compared to the previous year. It is anticipated that these threats will evolve and become more sophisticated in 2023, affecting companies, administrations, and users. Given this increase, six main types of cyberattacks can be identified: advanced malware, more sophisticated ransomware, improved phishing and smishing, intrusion techniques through home networks due to the rise of teleworking, the use of artificial intelligence for intrusion methods, and deepfakes—misleading messages created with artificial intelligence (IDET, 2022a). According to a Unisys security study based on national and international surveys of 11,000 adults aged 18 to 64 across 11 different markets, identity theft and bank card fraud are the primary concerns of Mexicans regarding cybersecurity. Despite 66% of respondents expressing distrust when clicking on suspicious links, only 29% were familiar with more sophisticated scams, such as SIM hijacking, and only 22% knew the appropriate organizations to report cyberattacks. In response to these challenges, the need to adopt biometric data to enhance user security and prevent attacks or data leaks has been highlighted (IDET, 2021).

The data indicate a concerning gender disparity in cyberbullying in Mexico, which affects a significant portion of the population, particularly women and girls. Of the victims

of digital violence, 95 out of 100 are women, while eight out of 10 aggressors are identified as men.

According to collected figures, approximately 9.8 million women aged 12 and over were victims of cyberbullying in 2022, compared to 7.6 million men in the same age group. Incidents are especially frequent among young women aged 20 to 29, with 29.3% reporting victimization in the past 12 months. Most acts of cyberbullying are perpetrated by strangers, accounting for 61.3% of cases, while 19.1% were committed by acquaintances. Furthermore, the most widely used digital platforms for cyberbullying are Facebook and WhatsApp, which constitute 44.5% and 45.5% of cases, respectively (Hernández, 2022). These figures highlight that cyberbullying poses a serious threat to the safety and well-being of individuals in Mexico, with a disproportionate impact on women and girls.

The phenomenon of violence has permeated schools in Mexico. Reports indicate that up to 60% of primary and secondary school teachers have been victims of violence from students, according to Dr. José Carlos Hernández, a specialist in Penal Systems and Criminal Policy. He highlights that only 17% of affected teachers dare to file a formal complaint with the authorities, mainly due to fear of retaliation from students' parents or the risk of losing their positions. The increase in violence is attributed to factors such as the lack of coherent public policies in education and the prevailing violence in students' family environments. Additionally, there is an urgent need to incorporate Axiology and Human Rights throughout the educational system to address this issue and restore the social fabric (González, 2024).

While physical and verbal violence against teachers currently receives greater attention due to its visibility and the nature of face-to-face interactions, it is important to note that teachers are also subject to cyberattacks from students, parents, and colleagues, although data on this matter is limited. The low percentage of complaints regarding acts of violence against teachers reflects an even more pronounced trend in the case of cyberattacks, exacerbated by the aggressors' lack of awareness and the unclear protocols to follow in such situations.

In a study of 162 surveyed teachers, it was found that only 16.8% admitted to having been victims of some form of cyberattack, with smartphones and tablets being the most common devices used in these incidents. Facebook was identified as the most frequently used platform for perpetrating cyberattacks, accounting for 86% of the recorded cases (Pereira, 2021).

Among the cyberattacks on teachers, sharing degrading material was found to be the most prevalent type, followed by "cyberbaiting"—provoking the teacher and recording his or her surprised reaction, mainly through mobile phones—and subsequently sharing these materials (Kopecký and Szotkowski, 2017, p. 2). Additionally, threats of intimidation or extortion were noted.A concerning trend observed in the study was the lack of response from teachers, with an alarming 86% choosing not to confront the situation, while only 13% decided to address the problem directly with the group. These results highlight the urgent need for implementing effective measures to protect teachers and to foster a safe and respectful school environment in the face of cyberviolence (Pereira, 2021). Definitions of cyberbullying are broad and diverse, making it difficult to determine whether an incident constitutes a one-time aggression or meets the criteria of repetition, duration, and perception of harm by the victim, as well as the presence of a power imbalance between the aggressor and the victim.

The conceptualization of cyberbullying is based on existing definitions of traditional bullying, which is perceived as aggressive, intentional, and repeated acts or behaviors directed against an individual or group that cannot easily defend themselves. Olweus (1993) emphasizes the need to distinguish between bullying and aggression, noting that aggression is seen as a one-time event, while bullying is characterized by a repeated phenomenon marked by a power imbalance between the aggressor and the victim (Olweus, 1993; Whitney and Smith, 1993; Rigby, 1997; Smith and Sharp, 1994). Thus, it can be said that the term cyberbullying logically extends the traditional definition of bullying, incorporating additional specificities, particularly in relation to information and communication technologies (ICT).

There is a multiplicity of definitions of cyberbullying, many of which are not compatible with one another. Some authors define it as any attack aimed at harming others in the online environment, while others argue that "true cyberbullying" must be deliberate, repeated, and intense (Juvonen and Gross, 2008; Patchin and Hinduja, 2006).

Among the most widely used definitions of cyberbullying is one that describes it as a deliberate, repeated, and harmful activity carried out using computers, mobile phones, and other electronic devices (Hinduja and Patchin, 2008; Patchin and Hinduja, 2006). Similarly, cyberbullying can be understood as any action conducted in cyberspace with the intention of insulting or humiliating others. Some definitions emphasize that it involves intentional and repeated harm caused by electronic means or messages (Juvonen and Gross, 2008; Hinduja and Patchin, 2008). This form of bullying behavior is often manifested when various social

networks, such as Facebook and Twitter, are used for open communication, and can be deliberately aimed at harming or harassing someone (Huang et al., 2014).

In addition, some definitions highlight the use of various media and technologies, such as email, text messages, phone calls, websites, and messaging and social networking applications, with the intention of harassing, threatening, humiliating, or attacking others, particularly adolescents (Li, 2007; Slonje and Smith, 2008; Dehue et al., 2009; Smith et al., 2008; Kowalski et al., 2012). Cyberbullying is experienced through emails, instant messages and communications, websites, online games, and also through messages or images sent to mobile phones (Kowalski et al., 2012).

The various definitions of cyberbullying reflect the complexity and breadth of the phenomenon, as well as the ongoing evolution of the ways in which it manifests in the digital environment. While all definitions agree on the characteristics of aggressive, intentional, and repeated behavior using information and communication technologies, there is a lack of consensus regarding the specificity of its traits and the severity of its effects. Additionally, accurate identification can be challenging due to its variable nature and the many ways it can manifest online.

Under these premises, the following research questions arise: What is the incidence of cyber violence directed from students to secondary school teachers in the state of Sinaloa, Mexico? What coping strategies do teachers use in response to this problem? What is the prevalence of cyberattacks faced by teachers? Who are the cyber attackers? These questions aim to understand the nature and incidence of the phenomenon, as well as the trends and patterns that may emerge from the collected data. Therefore, the following research objectives are derived from the aforementioned questions: to determine the incidence of cyber violence; to identify the coping strategies used by teachers; to assess the prevalence of cyberattacks faced by teachers; and to identify the perpetrators of cyberattacks directed at secondary school teachers in the state of Sinaloa, Mexico.

Cyberbullying to teachers

Teachers may become victims of bullying through malicious statements posted on social media (Tolentino, 2016). These practices on digital platforms often include insults related to the victims' intelligence, physical characteristics, and values (Hua et al., 2019; Zhao et al., 2016). For example, terms that portray someone as incompetent, reckless, or lacking intelligence may be used to demean their intellect. Additionally, "body-shaming" images that mock the victim's physical attributes, such as dark skin color or wrinkles, may be shared and

are now much more easily produced with the use of artificial intelligence. Online bullying experienced by teachers encompasses a variety of forms, ranging from the posting of obscene and edited images and audiovisual clips on fake Facebook pages to the dissemination of abusive, hurtful, and embarrassing comments against them. This can also include hacking their email accounts and spreading viruses, as well as offensive comments sent via emails, text messages, chat rooms, or websites (Eden et al., 2013; Garrett, 2014; Kauppi and Pörhölä, 2012a; Tolentino, 2016). In addition to these forms of online bullying, teachers may also face physical, verbal, and non-verbal bullying, as well as indirect bullying (James et al., 2008; Kauppi and Pörhölä, 2012b; Mooij, 2011). The inability of teachers to manage and discipline students, along with their strict behavior and low grading, are noted as significant causes of student bullying (De Wet, 2010). Furthermore, topics such as sexual harassment by university students towards young female teachers, as well as threats and defamation on social media experienced by teachers daily, raise additional concerns regarding bullying directed at educators.

Methodology

For this study, a quantitative research methodology with an exploratory scope was deemed appropriate since statistical analysis of the data can provide an objective understanding of the nature and magnitude of the problem of cyber violence against teachers in Sinaloa. These figures offer a solid foundation for the development of effective prevention and response policies and strategies.

Based on the above, it can be concluded that quantitative research explains phenomena by collecting detailed and consistent numerical data, which are analyzed using methods grounded in mathematics, particularly statistics. This approach raises questions about who, what, when, where, how much, how many, and how. It revolves around numbers, logic, and an objective stance (Mohaja, 2020).

In terms of scope, the research is both exploratory and descriptive. As the term implies, it aims to explore the research questions rather than provide definitive and conclusive solutions to existing problems. This type of research is generally conducted to investigate a problem that has not yet been clearly defined, allowing for a better understanding of its nature (Dudovskiy, 2022).

The research is also descriptive in scope, as it is based on a prior understanding of the characteristics of the phenomenon in question, similar to the approach taken by Pereira

(2021). It focuses on the exposition and description of aspects present in a specific group of individuals, such as teachers in the State of Sinaloa. Within the context of quantitative descriptive research, statistical data analysis is employed to examine central tendencies and variability. While it is possible to formulate hypotheses to characterize the studied phenomenon, these hypotheses are not considered essential requirements in this type of research (Ramos, 2020).

A survey was utilized as the research technique. Pinsonneault and Kraemer (1993, as cited in Glasow, 2005) defined a survey as a "means of collecting information about the characteristics, actions, or opinions of a large group of people" (p. 77). Surveys can also be used to assess needs, demands, and impact (Salant and Dillman, 1994, p. 2, as cited in Glasow, 2005). This instrument was validated using the judge validation technique.

According to Corral (2009), validation implies that an instrument must accurately and representatively capture a specific domain of the content related to the characteristic or trait being assessed. This process seeks to determine the extent to which the items or questions of an instrument adequately reflect the universe of content associated with the characteristic or trait in question. Regarding reliability, it refers to the degree of precision and accuracy in the measurement process.

The approval of the content, facilitated by an expert report, was conducted in a methodical and enlightening manner, achieving consensus among the judges. The survey used in this research addressed five significant variables: sociodemographic data, training, Internet safety, cyber violence directed by students towards teachers (both personal experiences and observations), and coping strategies. The instrument consisted of 33 questions distributed across these five factors. Once the work was completed, Friedman's F test was found to be useful in confirming the findings related to the research group (González and Pereira, 2023).

In Sinaloa, there is a total population of 13,258 secondary school teachers, of which 7,402 work in state secondary schools. These state schools are divided into public and private institutions, with 5,725 teachers in public schools and 1,677 in private schools (National Institute of Statistics and Geography [INEGI], 2023).

To determine the valid sample size, several factors needed to be considered, including the relationship between the sample size and the total population, as well as the sampling technique employed. In this case, the total population consists of 7,402 teachers, and a sample of 961 was selected. To assess the validity of the sample, the sampling error was calculated using the appropriate formula: $E=((z\sqrt{(p(1-p)))}/N)/\sqrt{n}$

Therefore, the sampling error is approximately 0.000336, which indicates that the margin of error for the sample is very small compared to the population size. It can be concluded that, with a confidence level of 95%, the sample of 961 teachers is valid for representing the total population of 7,402 teachers.

From the sample of 961 teachers from state secondary schools in Sinaloa, the distribution by type of school was as follows: 852 teachers (88.7%) were from public schools, while 109 teachers (11.3%) were from private schools. Regarding the distribution by gender, the sample included a higher proportion of women (544 or 56.7%) than men (414 or 43.2%).

Regarding the distribution of the teachers surveyed by age group, the following results were obtained: 135 teachers (14%) are between 20 and 30 years old, 384 teachers (40%) are between 31 and 40 years old, 299 teachers (31.1%) are between 41 and 50 years old, 133 teachers (13.8%) are between 51 and 60 years old, and 13 teachers (1.4%) are over 61 years old. In terms of years of service, the sample revealed that 236 teachers (24.6%) had between zero and five years of experience, 279 teachers (29%) had between six and ten years, 259 teachers (27%) had between eleven and twenty years, 159 teachers (16.5%) had between twenty-one and thirty years, 30 teachers (3.1%) had between thirty-one and forty years, three teachers (0.3%) had between forty-one and fifty years, and one teacher (0.1%) had between fifty-one and sixty years. Regarding educational level, it was found that 648 teachers (67.6%) have a Bachelor's degree, 84 teachers (8.8%) are Bachelor's interns, 80 teachers (8.3%) are Master's graduates, 97 teachers (10.1%) are Master's interns, 13 teachers (1.4%) are PhD graduates, 23 teachers (2.4%) are PhD interns, and 14 teachers (1.5%) have only completed high school.

The sample shows a predominance of teachers working in public schools, a higher proportion of women compared to men, a wide yet concentrated age distribution in the middle stages of their teaching careers, and a mix of experienced and relatively new teachers in terms of years of service. Additionally, the majority of the teachers hold at least a Master's degree, indicating a relatively high educational level.

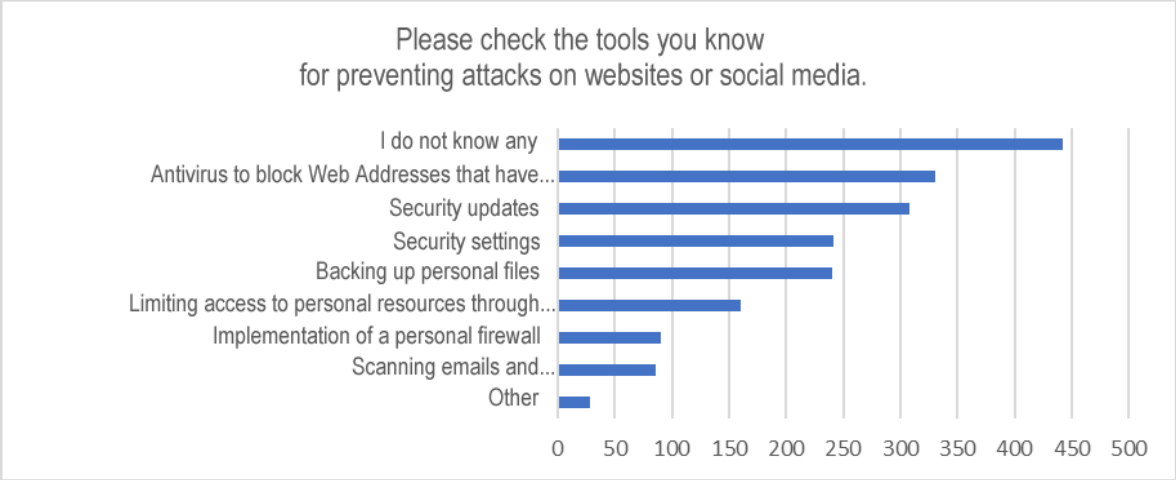
The setting, the state of Sinaloa, according to the General Directorate of Planning, Programming, and Educational Statistics of the Ministry of Public Education (DGPPYEE-SEP, 2023), covers a territorial area of 57,365 km² and has a population of 3,026,943 inhabitants. This represents approximately 2.9% of the national territory and 2.4% of the total population of Mexico. The gender distribution in Sinaloa is relatively balanced, with 50.6% women and 49.4% men. Regarding education, for the 2021-2022 school year, Sinaloa had a total enrollment of 869,881 students, of which 50.8% are women and 49.2% are men. This

enrollment represents approximately 2.5% of the total in the National Education System. The distribution of enrollment by educational level shows that 69.6% corresponds to basic education, 15.6% to upper secondary education, and 14.7% to higher education. In terms of educational coverage, it is observed that preschool education has a coverage rate of 70.4%, with attention varying by age group between 52.8% and 90.9%. In primary education, coverage reaches 97.9%, with a net enrollment rate of 92.4% and a school dropout rate of 0.1%. In secondary education, coverage is 94.9%, with a school dropout rate of 3.0%.

Analysis of results

The first set of results pertains to security measures, emphasizing the importance of security updates and the use of antivirus software. Additionally, it highlights the need to raise awareness of other preventive measures, such as scanning emails, limiting access on mobile devices, and implementing personal firewalls, as illustrated in Figure 1 below.

Figure 1. Cybersecurity Tools.



Source: Own Elaboration.

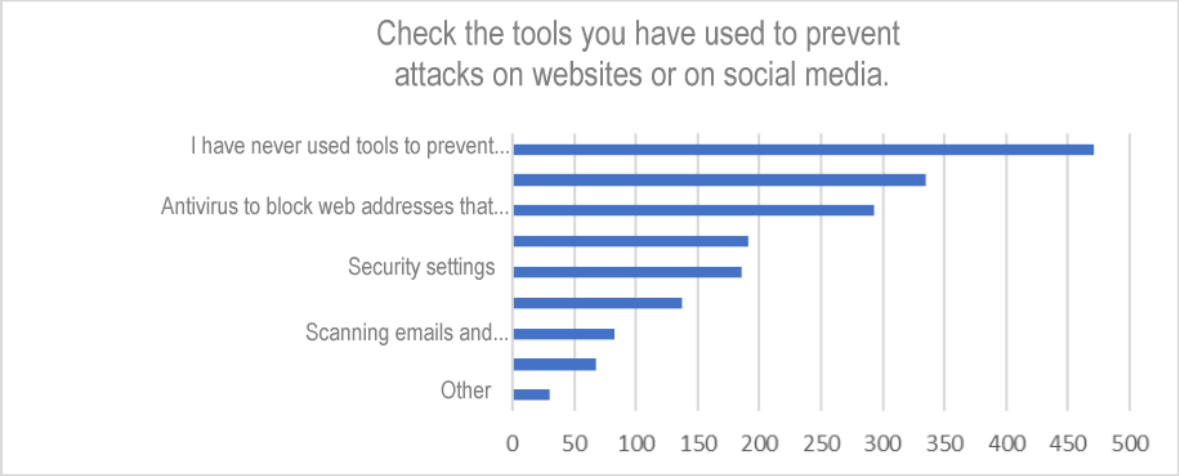
Regarding the level of security awareness, the fact that 46% of respondents indicated they were unaware of any specific tools to prevent attacks on websites or social networks suggests a concerning lack of awareness about cybersecurity. This highlights the need for education and awareness regarding the importance of online security.

However, in terms of the prevalence of security tools, the responses indicate their recognition as effective preventive measures, reflecting a basic understanding of online security practices. Additionally, other aspects underscore the importance of promoting a broader and more diversified cybersecurity culture. It is crucial to educate teachers about the

significance of taking proactive measures to protect their online security and privacy. It should also be noted that "other" responses pertained to activities related to security settings.

The results reveal a variety of security measures employed by respondents, with a particular emphasis on security updates and the use of antivirus software. However, there is a need to raise awareness of additional preventive measures, such as scanning emails and limiting access on mobile devices. The responses to the question regarding the tools used to prevent attacks on the web or social networks also indicate a concerning correlation with the reasons for cyber violence attacks, as illustrated in Figure 2.

Figure 2. Tools Used by Teachers to Prevent Cyberattacks.



Source: Own Elaboration.

A lack of knowledge about online security tools—reported by 46% of respondents—contributes to individuals' vulnerability to cyber violence attacks. Insufficient awareness of how to protect themselves online exposes people to the risks of online violence, which underscores the necessity for ongoing cybersecurity training for teachers.

The relationship between the data on the tools respondents are familiar with and the tools they actually use can provide valuable insights into the awareness, adoption, and effectiveness of online security measures. There may be a positive correlation between knowledge and the use of online security tools; that is, respondents who are familiar with a broader range of security tools are more likely to use them compared to those who are familiar with fewer options.

On the other hand, it is also possible that there is a negative correlation between knowledge of security tools and their actual use. Respondents may be familiar with various security tools but might choose not to use them for several reasons, such as the complexity of configuration, a lack of confidence in their effectiveness, or simply a lack of interest in

online security. Furthermore, respondents may be acquainted with a wide range of security tools but only utilize a subset of them, or they might be using antivirus software without fully understanding how it works or what other security measures are available. What is particularly concerning is that almost half of the respondents (46%) claim to be unaware of any specific tools to prevent online attacks, indicating a significant lack of awareness or education regarding the security measures available. This gap in knowledge could leave these individuals more vulnerable to cyberattacks. The data gathered when respondents were asked if they had ever been victims of cyberattacks or cyberbullying by a student or group of students at their workplace reveal interesting trends and perceptions about the incidence of educational cyberattacks, both from the teachers' perspective and regarding students' perceptions of cases involving teachers. Notably, 788 respondents (82%) answered 'no,' 99 (10.3%) were unsure, and 74 (7.7%) reported knowing of cases. However, when asked if they were aware of any cases of cyberattacks or cyberbullying by students towards teachers, the percentages changed: 274 (28.5%) stated that they knew of cases, 93 (9.7%) were unsure, and 594 (61.8%) indicated that they were unaware of any such incidents.

Based on personal experience, the fact that 82% of the surveyed teachers reported never having been victims of cyberattacks or cyberbullying by students is a positive indication regarding the perception of security in the workplace. However, it is important to note that a small percentage (7.7%) did report being victims, which indicates that these issues exist within educational environments.

Regarding awareness of cases, the significant increase in the percentage of teachers who reported knowing about cases of cyberattacks or cyberbullying by students towards teachers (28.5%) is noteworthy. This highlights that, although some teachers may not have personally experienced these attacks, they are aware that such problems may be occurring in their work environment.

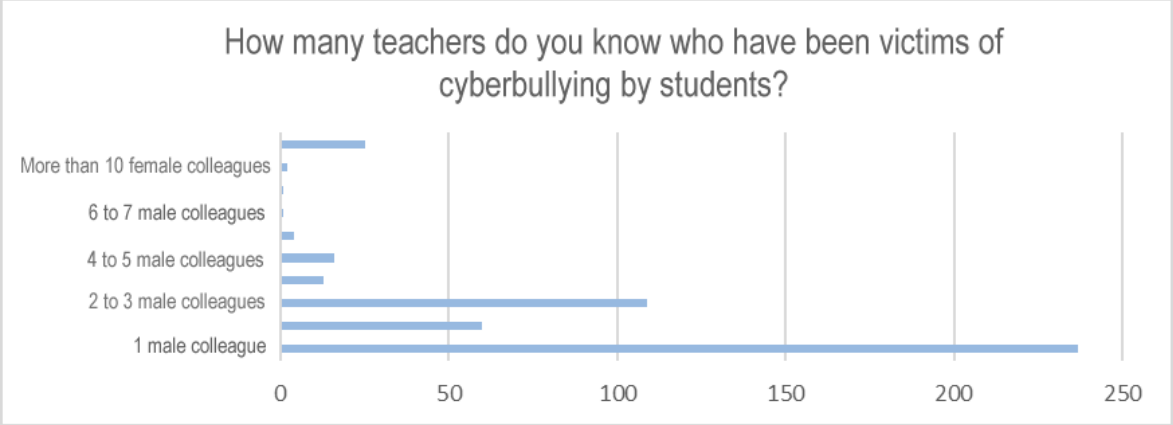
In terms of perceived safety, the discrepancy between the percentage of teachers who reported not having been personally victimized (82%) and those who are aware of cases of cyberattacks or cyberbullying targeting teachers (28.5%) may suggest that some teachers underestimate the prevalence of these issues in their workplace. This has implications for teachers' perception of safety and well-being in the educational setting.

In terms of awareness and sensitivity, the fact that a significant number of teachers are uncertain (10.3% and 9.7%, respectively) about whether they have been victims or are aware of cases of cyberattacks or cyberbullying underscores the need to enhance awareness and sensitivity regarding these issues within the educational environment.

The data suggest that, while the majority of teachers may not have been directly affected by cyberattacks or cyberbullying, there is a widespread recognition of the existence of these problems in educational settings. This underscores the importance of implementing preventive and supportive measures to ensure a safe and healthy work environment for all members of the educational community.

Those who were aware of cases of cyberattacks on teachers were instructed to proceed to the next section, and 467 respondents (48%) did so, indicating that nearly half of the participants were aware of such incidents. When asked if they knew anyone who had been a victim, the data revealed that a small percentage of teachers reported knowing a significant number of colleagues who have experienced cyberbullying, including instances involving more than 10 colleagues. This highlights the seriousness of the issue, as illustrated in Figure 3.

Figure 3. Teachers Known to Have Suffered Cyberbullying



Source: Own Elaboration.

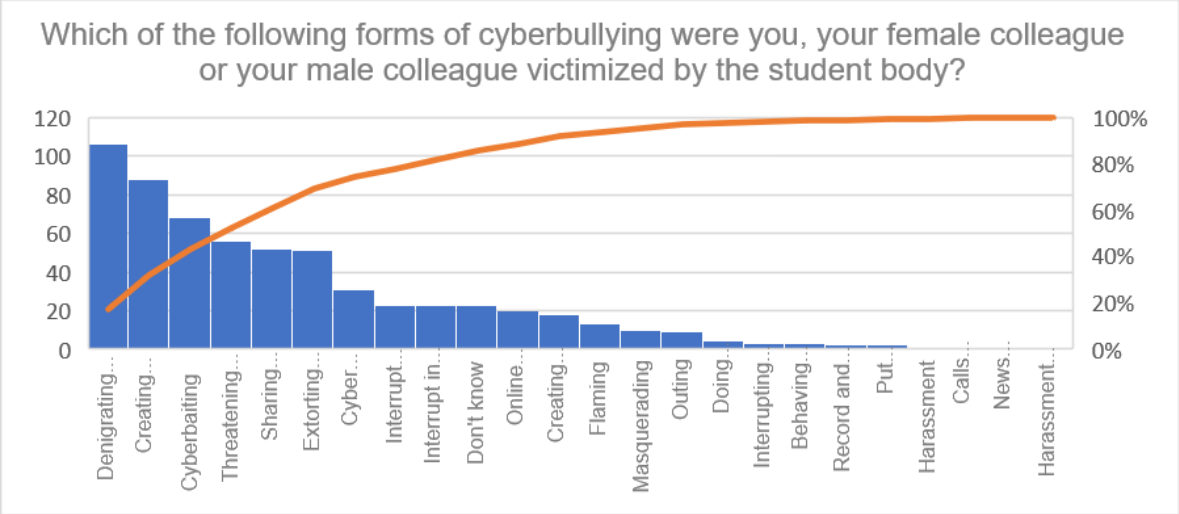
The data indicate that cyberbullying is a significant concern within the educational environment and affects a notable percentage of teachers. The frequency of cyberbullying victims by gender is particularly highlighted; while 363 respondents (77%) reported knowing colleagues who were victims, only 79 (16.9%) reported knowing female teachers who had been targeted.

A marked disparity in incidence is evident between male and female teachers. This gender gap suggests that male teachers are experiencing a higher number of cyber violence cases compared to their female counterparts, indicating that men may be more likely to be the targets of cyberattacks in this specific context, particularly at the secondary education level. Additionally, there may be differences in how male and female teachers perceive cyber

violence. Men may be more inclined to identify and report incidents they experience, while women may underreport, fail to acknowledge, or refrain from commenting on or reporting certain behaviors.

In response to the question, "Which of the following forms of cyberbullying were you or your fellow teachers subjected to by students?", teachers were asked to check all forms of cyberattacks they were aware of. Figure 4 reveals the various ways in which teachers can become victims, underscoring the importance of addressing this issue appropriately and promoting a safe and respectful online environment for all members of the educational community.

Figure 4. Forms of Cyberbullying from the student to the teacher.



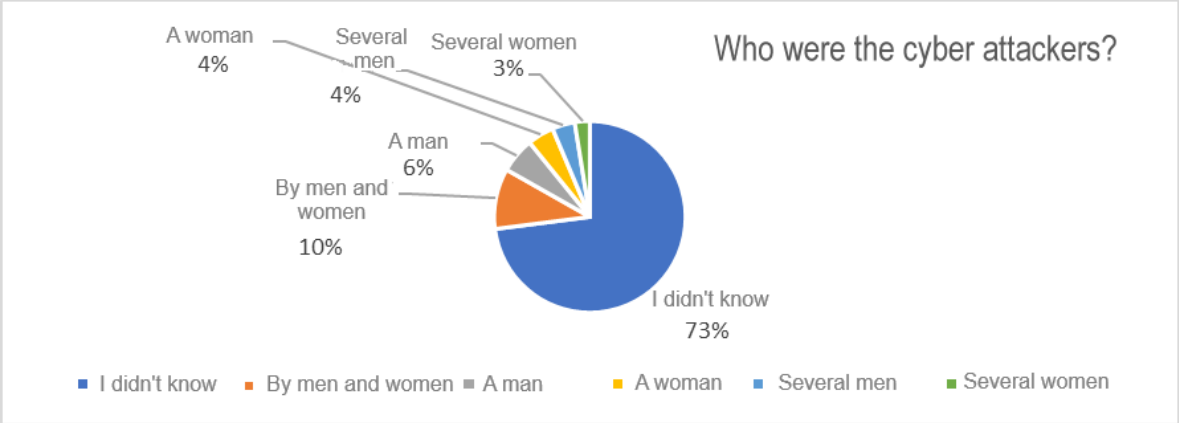
Source: Own Elaboration.

In Figure 4, the frequency of each form of cyberbullying mentioned is illustrated. The five most common forms are as follows: first, denigrating individuals by publishing harmful or false stories, photos, or videos, with 106 reported cases; second, creating false profiles, which accounted for 88 cases; third, cyberbaiting—deliberately provoking negative reactions online—with 68 cases reported; fourth, online threats and intimidation, with 56 reports; and fifth, sharing degrading material, which had 52 reports.

It is worth noting that online extortion or threats occupied sixth place with 51 cases, and online threats and intimidation were mentioned twice in the previous statement, suggesting an error to clarify. These figures indicate a serious problem regarding the use of cell phones, particularly as teachers frequently create WhatsApp groups, making them vulnerable to threats, intimidation, and extortion.

When asked about the identity of the cyber attackers, the data revealed that a majority of respondents could not clearly identify them. However, it is noteworthy that both men and women, as well as individuals acting alone or in groups, can be involved in cyberattacks, as shown in Figure 5.

Figure 5. Identification of teachers' cyber attackers.



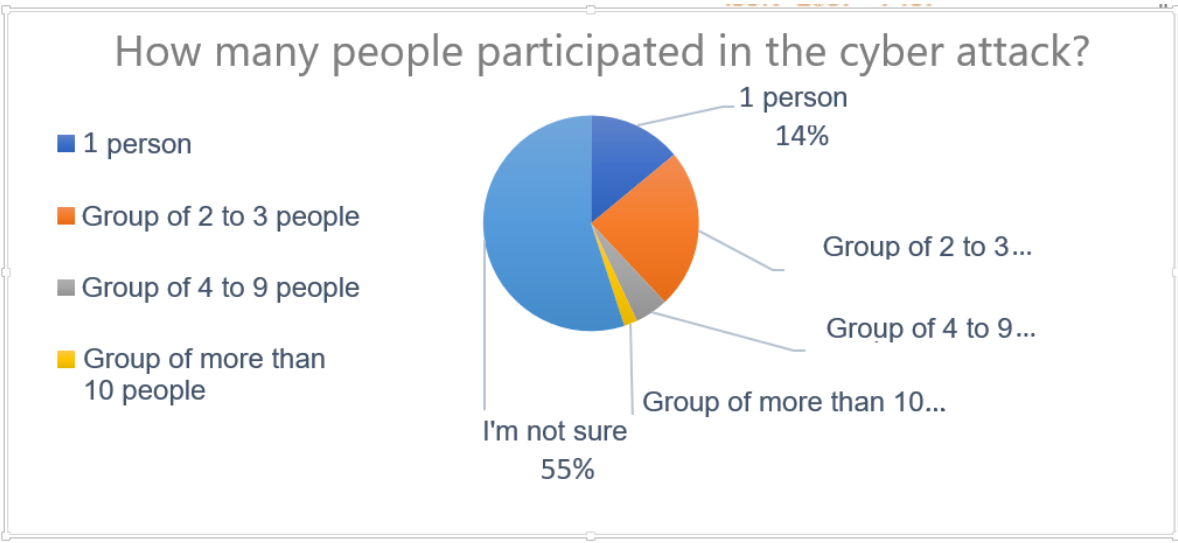
Source: Own Elaboration.

In Figure 4, the frequency of each form of cyberbullying is illustrated. The five most common forms are as follows: first, denigrating individuals by publishing harmful or false stories, photos, or videos, which accounted for 106 reported cases; second, creating false profiles, with 88 cases; third, cyberbaiting—deliberately provoking negative reactions online—with 68 reported cases; fourth, online threats and intimidation, with 56 reports; and fifth, sharing degrading material, which had 52 reports.

It is important to note that online extortion occupied sixth place with 51 cases. The repeated mention of online threats and intimidation suggests a need for clarification. These figures indicate a serious problem related to the use of cell phones, particularly as teachers frequently create WhatsApp groups, leaving them vulnerable to threats, intimidation, and extortion.

When asked about the identity of cyber attackers, the data revealed that a majority of respondents could not clearly identify them. However, it is noteworthy that both men and women—as well as individuals acting alone or in groups—can be involved in cyberattacks, as illustrated in Figure 5

Figure 6. Number of people who participated in cyber attacks on teachers.

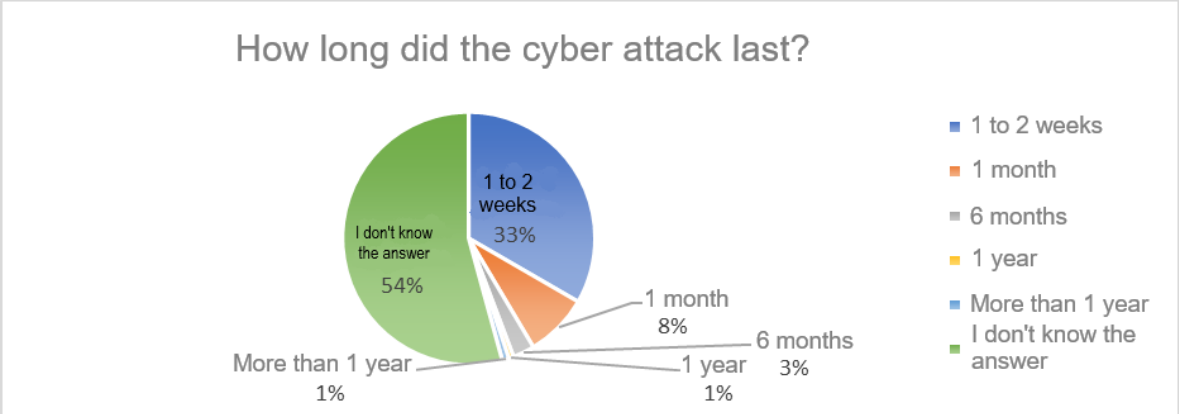


Source: Own Elaboration.

The diversity of cyberattack incidents on teachers is proportional to the distribution of responses, given the wide variety in perceptions about the nature of cyberattacks; while some perceive the attacks as being carried out by groups of various sizes, others consider them to have been perpetrated by lone individuals.

When questioned about the duration of the cyberattack, the findings obtained are worrying given that some cases were prolonged for significant periods, as seen in Figure 7.

Figure 7. Permanence of the cyber attack.



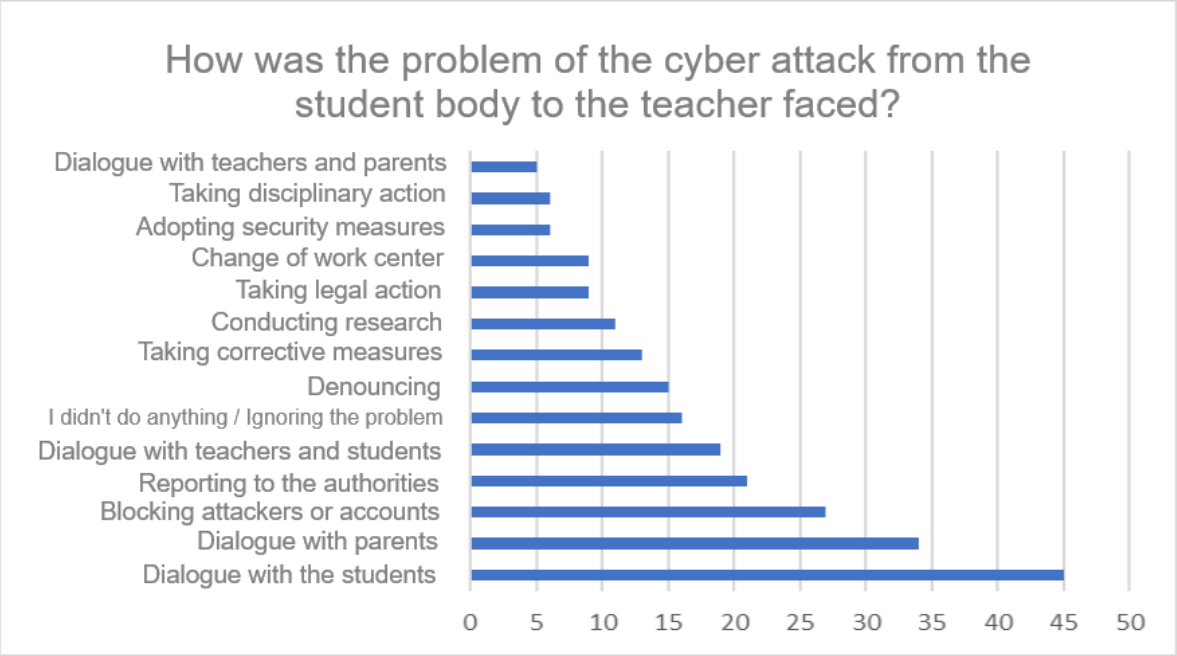
Source: Own Elaboration.

The data suggest that cyberattacks directed at teachers by students can vary significantly in duration, ranging from relatively short periods to more prolonged situations. Notably, a considerable number of respondents reported being unaware of the duration of the cyberattacks, indicating that these incidents may go unnoticed or remain poorly understood

by the affected teachers. Additionally, most respondents indicated that the cyberattacks lasted between one and two weeks; however, there were cases that extended for months or even more than a year, underscoring the seriousness and persistence of these issues.

The following results offer insights into how teachers addressed these problems, revealing a variety of strategies employed in response to cyberattacks within the school environment. First, dialogue—direct communication with students—emerged as a fundamental strategy, chosen as a means of personally resolving the issue and avoiding the involvement of other parties in the educational context, as shown in Figure 8.

Figure 8. Teacher's coping with student cyber attacks.



Source: Own Elaboration.

The primary strategies teachers employ to confront the issue include talking with students (45 responses), communicating with parents (34 responses), and blocking the attackers' accounts or their own (27 responses). It is concerning to note that some teachers have had to change their workplace (9 cases) or were fired as a result of being victims of cyberattacks by students (1 case). Additionally, there were instances where teachers felt powerless or chose to ignore the problem (16 cases). However, some cases were reported to or communicated by school authorities (21 cases each).

These findings collectively underscore the complexity and seriousness of the challenges teachers face regarding school cybersecurity.

Discussion

While cyberbullying among students has been extensively researched, there is growing concern regarding its impact on teaching staff, making it a relatively new topic that has been little studied. Research conducted by Challenor (2019), as well as by Rajbhandari and Rana (2022), along with data collected in Sinaloa, Mexico, reveal a troubling trend in the increasing incidence of cyberbullying against teachers across various geographical contexts.

In the Czech study by Kopecký and Szotkowski (2017), a prevalence rate of 21.73% was found among the surveyed teachers, primarily comprising primary and secondary school educators. In contrast, the study conducted in Sinaloa reported a higher prevalence of 33.7%, indicating a greater awareness of or victimization among teachers, with instances of both male and female victims. Conversely, Challenor's (2019) research in Ireland indicated a lower prevalence rate of 9.5%, suggesting that a minority of post-primary teachers had experienced cyberbullying.

All three studies identify a range of cyberattack forms targeting education professionals, including cyberbaiting, flaming, cyber-stalking, and the creation of fake profiles. Each investigation documents cases of online harassment, defamation through harmful or false content, as well as threats and intimidation. Intrusion into personal accounts and identity theft are also concerning issues highlighted in these studies. Furthermore, there is a noticeable trend toward disruption of the educational environment, with instances of disruptors interrupting virtual classes with obscenities and sharing inappropriate content on messaging platforms. In Sinaloa, online extortion, threats, and intimidation, particularly through the use of WhatsApp groups, pose serious problems in the teaching context.

Regarding coping strategies, Challenor (2019) identifies several approaches, including ignoring the problem, imposing technological limits to protect privacy, and restricting students' access to personal social networks. Rajbhandari and Rana (2022) observe a variety of responses ranging from ignorance of the issue to seeking legal support, changing jobs, or employing coping strategies such as deactivating social media accounts and staying invisible for a period. Conversely, the study in Sinaloa emphasizes dialogue as the primary coping strategy, whether with students, parents, or colleagues. While blocking and reporting to authorities are also common practices, the initial focus is often on communication and conflict resolution.

One notable coping strategy highlighted by Rajbhandari and Rana (2022), which was not employed by the teachers studied in Sinaloa, is the practice of keeping records and evidence of the cyberbullying incidents. This documentation could be crucial for supporting future actions and should be encouraged as part of a teacher's routine.

Concerning the duration of cyberattacks, Challenor's (2019) study found significant variability. For instance, two teachers experienced cyberattacks lasting one to two weeks, while one reported an attack lasting six months, and eight teachers indicated that the duration exceeded one year. Similarly, in Sinaloa, the duration of cyberattacks varied widely: there were 156 cases lasting one to two weeks, 38 lasting one month, 13 lasting six months, three lasting one year, and four lasting more than one year. Moreover, a substantial number of respondents (254) indicated they did not know the duration of the attacks.

Conclusion

The data presented in this research offer a detailed perspective on the issue of cyber violence against teachers in the state of Sinaloa. It highlights the security measures implemented, the coping strategies employed by affected individuals, and the types of perpetrators involved. These findings underscore the pressing need for greater awareness and training related to cybersecurity in the educational sector, as well as the establishment of effective protocols and policies to address instances of cyber violence directed from students towards teachers.

The research reveals a significant prevalence of cyberattacks and cyberbullying against educators, with notable disparities in incidence between genders. While most teachers may not have directly experienced these issues, there exists widespread awareness of their presence within the educational environment.

The findings confirm the initial assumption regarding the lack of knowledge about online security tools among teachers, which exacerbates their vulnerability to cyberattacks. Teacher self-protection is crucial; educators must first be equipped to defend themselves in order to effectively safeguard their students in cyberspace. Therefore, it is imperative to provide teachers with the necessary resources and support to confront these challenges. If educators are unfamiliar with how to protect their own online security, it becomes increasingly challenging for them to teach cybersecurity effectively to their students.

Addressing the knowledge gap, previous studies have not thoroughly examined the relationship between teachers' knowledge and their use of online security tools, nor have they

explored the incidence of cyberattacks in relation to teachers' gender. This study contributes to the field by providing empirical data that underscore the importance of tackling this problem comprehensively and proactively.

Throughout the research, it was noted that some teachers were uncertain whether they had been victims of cyberattacks or were aware of such incidents happening to others, indicating a lack of awareness or recognition of the problem. Additionally, the need for specific policies and measures to combat cyberbullying in educational settings was emphasized, making this a significant contribution of the study.

However, a limitation of this research is the lack of long-term follow-up concerning the psychological effects on victims, as well as teachers' perceptions of cyberattacks and descriptions of their experiences.

Future lines of research

The results of this research prompt new questions regarding the incidence of cyber violence against secondary school teachers in other states, its prevalence across different educational levels, the relationship between knowledge and the adoption of online security measures, and how factors such as age and experience influence perceptions and responses to the issue.

It is recommended that future studies conduct surveys of cyberbullying victims to evaluate the long-term psychological effects and the effectiveness of coping strategies employed by affected teachers. Additionally, research should explore teachers' perceptions of cyberattacks and their lived experiences, taking into account factors such as work-related stress, anxiety, and emotional well-being.

Moreover, the development and evaluation of specific intervention protocols to address cyberbullying in educational settings is essential. These protocols should include preventive measures, support resources, and response strategies for addressing incidents of cyber violence.

Finally, it would be crucial to investigate the effectiveness of cyberbullying prevention policies and strategies in schools, as well as to implement digital education programs aimed at promoting safe and responsible technology use among both students and teaching staff. Such efforts are vital in combating this growing issue within the educational field.

References

Challenor, L. P. (2019). *The Cyberbullying of Post-Primary Teachers in Ireland* [Doctoral dissertation]. Institute of Education, Dublin City University. https://doras.dcu.ie/23733/1/Liam%20Challenor%20PhD%20DORAS%20Copy.pdf

Corral, Y. (2009). Validez y confiabilidad de los instrumentos de investigación para la recolección de datos. *Revista Ciencias de la Educación, 19*(33), 228-247. https://bit.ly/3HcZjOA

Dehue, F., Koeter, M. W., & Schaufeli, W. B. (2009). Pesten op het werk: de relatie met gezondheid en verzuim en de rol van coping. *Gedrag y Organisatie, 22*(2), 97-117. https://doi.org/10.5117/2009.022.002.001

De Wet, C. (2010). Victims of educator-targeted bullying: A qualitative study. *South African Journal of Education, 30*(2). https://doi.org/10.15700/saje.v30n2a341

Dirección de Estudios de Política Educativa, Dirección General de Planeación, Programación y Estadística Educativa- Secretaría de Educación Pública (DGPPYEE-SEP). (2023). *Atlas de los servicios educativos: Representación cartográfica del acceso y prestación de los servicios educativos en México*. (Primera edición). SEP. https://www.planeacion.sep.gob.mx/Doc/Atlas_estados/0000_Atlas_completo.pdf

Dudovskiy, J. (2022). *The Ultimate Guide to Writing a Dissertation in Business Studies: A Step-by-Step Assistance*. (6th ed.). Research Methodology. https://www.scirp.org/reference/referencespapers?referenceid=3477576

Eden, S., Heiman, T., & Olenik-Shemesh, D. (2013). Teachers' perceptions, beliefs and concerns about cyberbullying. *British Journal of Educational Technology, 44*(6), 1036–1052. https://doi.org/10.1111/j.1467-8535.2012.01363.x

Garrett, L. (2014). The student bullying of teachers: an exploration of the nature of the phenomenon and the ways in which it is experienced by teachers. Aigne, (5) 19-40. https://www.ucc.ie/en/media/electronicjournals/aigne/2014-01/03-Garrett-2014-01-en.pdf

Glasow, P. A. (2005, April). Fundamentals of Survey Research Methodology. *Report No. 25988 of Washington C3 Center, McLean, Virginia: MITRE Department.* Division: Department: W800 W804. https://www.mitre.org/sites/default/files/pdf/05_0638.pdf

González, V. (20 de marzo de 2024). Sufren 60% de los maestros violencia por parte de sus alumnos: especialista. *El Heraldo de Chihuahua.*

https://www.elheraldodechihuahua.com.mx/local/chihuahua/sufren-60-de-los-maestros-violencia-por-parte-de-sus-alumnos-especialista-10064719.html

González Torres, A. y Pereira Hernández, M. L. (2023). Encuesta: ciberviolencia dirigida al docente a través de una examinación de autenticidad por dictamen de árbitros. *Revista Internacional de Investigación en Didáctica de las Ciencias y la Matemática, 13*(26). https://doi.org/10.23913/ride.v13i26.1432

Hernández Oropa, M. (2022). Informe violencia digital. Las sociedades patriarcales creamos víctimas y agresores. Un informe para entender cómo, dónde y quiénes perpetúan de forma sistémica la violencia virtual contra las mujeres y niñas en México. Frente Nacional para la Sororidad y Defensoras Digitales.https://leyolimpia.com.mx/wp-content/uploads/2022/12/FNSDG_Reporte2022_DICIEMBRE2022.pdf

Hinduja, S., & Patchin, J. W. (2008). Cyberbullying: An exploratory analysis of factors related to offending and victimization. *Deviant Behavior, 29*, 129-156. https://doi.org/10.1080/01639620701457816

Hua, T. K., So'od, S. M. M., & Hamid, B. A. (2019). Communicating insults in cyberbullying. *Journal of Media and Communication Research, 11*(3), 91-109. https://fslmjournals.taylors.edu.my/wp-content/uploads/SEARCH/SEARCH-2019-11-3/SEARCH2019-P6-11-3.pdf

Huang, Q., Singh, V. K., & Atrey, P. K. (2014). Cyber Bullying Detection Using Social and Textual Analysis. *Proceedings of the 3rd International Workshop on Socially-Aware Multimedia, Orlando, Florida, USA*. https://doi.org/10.1145/2661126.2661133

Instituto del Derecho de las Telecomunicaciones (IDET). (18 de noviembre de 2022). *México está en riesgo por ciberataques, dice Monreal.* IDET (Ed.). https://www.idet.org.mx/noticias/mexico-esta-en-riesgo-por-ciberataques-dice-monreal

Instituto del Derecho de las Telecomunicaciones (IDET). (18 de octubre de 2021). *Mexicanos, los más preocupados.* IDET (Ed.). https://www.idet.org.mx/noticias/mexicanos-los-mas-preocupados

Instituto del Derecho de las Telecomunicaciones (IDET). (23 de noviembre de 2020). *México: 10 mil ciberataques al mes.* IDET (Ed.). https://www.idet.org.mx/noticias/mexico-10-mil-ciberataques-al-mes/

Instituto del Derecho de las Telecomunicaciones (IDET). (27 de diciembre de 2022a*). Los 6 ciberataques que serán más habituales en 2023.* IDET (Ed.). https://www.idet.org.mx/noticias/los-6-ciberataques-que-seran-mas-habituales-en-2023/

Instituto Nacional de Estadística y Geografía (INEGI). (2023). *Maestros y escuelas por entidad federativa según nivel educativo, ciclos escolares seleccionados de 2000/2001 a 2022/2023* [Datos interactivos]. https://www.inegi.org.mx/app/tabulados/interactivos/?pxq=8c29ddc6-eeca-4dcc-8def-6c3254029f19

James, D. J., Lawlor, M., Courtney, P., Flynn, A., Henry, B., & Murphy, N. (2008). Bullying behaviour in secondary schools: What roles do teachers play? *Child Abuse Review, 17*(3), 160-173. https://doi.org/10.1002/car.1025

Juvonen, J., & Gross, E. F. (2008). Extending the school grounds? Bullying experiences in cyberspace. *Journal of School Health, 78*(9), 496-505. https://doi.org/10.1111/j.1746-1561.2008.00335.x

Kauppi, T., & Pörhölä, M. (2012a). School teachers bullied by their students: Teachers' attributions and how they share their experiences. *Teaching and Teacher Education, 28*(7), 1059-1068. https://doi.org/10.1016/j.tate.2012.05.009

Kauppi, T., & Pörhölä, M. (2012b). Teachers bullied by students: Forms of bullying and perpetrator characteristics. *Violence and Victims, 27*(3), 396-413. https://doi.org/10.1891/0886-6708.27.3.396

Kopecký, K., & Szotkowski, R. (2017). Cyberbullying, cyber aggression and their impact on the victim – The teacher. *Telematics and Informatics, 34*(2), 506-517. https://doi.org/10.1016/j.tele.2016.08.014

Kowalski, R. M., Limber, S. P., & Agatston, P. W. (2012). *Cyberbullying: Bullying in the digital age* (2nd ed.). Wiley Blackwell. https://psycnet.apa.org/record/2012-04615-000

Li, Q. (2007). New bottle but old wine: A research of cyberbullying in schools. *Computers in Human Behavior, 23*(4), 1777-1791. https://doi.org/10.1016/j.chb.2005.10.005

Mohajan, H. K. (2020). Quantitative Research: A Successful Investigation in Natural and Social Sciences. *Journal of Economic Development, Environment and People, 9*(4), 52-79. https://mpra.ub.uni-muenchen.de/105149/

Mooij, T. (2011). Secondary school teachers' personal and school characteristics, experience of violence and perceived violence motives. *Teachers and Teaching: Theory and Practice, 17*(2), 227-253. https://doi.org/10.1080/13540602.2011.539803

Olweus, D. (1993). *Bullying at school: What we know and what we can do*. Blackwell Publishers.

Patchin, J., & Hinduja, S. (2006). Bullies move beyond the schoolyard: A preliminary look at cyberbullying. *Youth Violence and Juvenile Justice, 4*(2), 123-147.

Pereira Hernández, M. L. (2021). El docente de secundaria: Una víctima más de los ciberataques. En *Memoria electrónica del XVI Congreso Nacional de Investigación Educativa.* https://www.comie.org.mx/congreso/memoriaelectronica/v16/doc/1404.pdf

Pereira Hernández, M. L. (2023). Violencia al docente: Una revisión sistémica de la circulación del conocimiento. *Dilemas Contemporáneos: Educación, Política y Valores, 10*(3), Artículo no. 45. https://dilemascontemporaneoseducacionpoliticayvalores.com/index.php/dilemas/article/view/3628

Pereira Hernández, M. L. (2024). *Voces silenciadas: Desvelando la violencia y ciberviolencia hacia docentes en estudios de acceso abierto*. Universidad Tecnológica de Puebla. https://doi.org/10.58299/utp.186

Ramos-Galarza, C. A. (2020). Los alcances de una investigación. *CienciAmérica, 9*(3), 1–6. https://doi.org/10.33210/ca.v9i3.336

Rajbhandari, J., & Rana, K. (2022). Cyberbullying on Social Media: An Analysis of Teachers' Unheard Voices and Coping Strategies in Nepal. *International Journal of Bullying Prevention, 5*, 95-107. https://doi.org/10.1007/s42380-022-00121-1

Rigby, K. (1997). Attitudes and beliefs about bullying among Australian children. Irish *Journal of Psychology, 18*, 202-209.

Slonje, R., & Smith, P. K. (2008). Cyberbullying: Another Main Type of Bullying? *Scandinavian Journal of Psychology, 49*, 147-154. https://doi.org/10.1111/j.1467-9450.2007.00611.x

Smith, P. K., & Sharp, S. (1994). *School Bullying: Insights and Perspectives.* Routledge.

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. *Journal of Child*

Psychology and Psychiatry, 49(4), 376-385. https://doi.org/10.1111/j.1469-7610.2007.01846.x

Tolentino, A. C. (2016). Bullying of a teacher in the workplace: A phenomenological study. *International Journal of Learning and Teaching, 2*(1), 20-27. https://doi.org/10.18178/ijlt.2.1.20-27

Whitney, I., & Smith, P. K. (1993). A survey of the nature and extent of bullying in junior/middle and secondary schools. *Educational Research, 35*(1), 3-25. https://doi.org/10.1080/0013188930350101

Zhao, R., Zhou, A., & Mao, K. (2016). Automatic detection of cyberbullying on social networks based on bullying features. *Proceedings of the 17th international conference on distributed computing and networking*, Singapore. https://doi.org/10.1145/2833312.284956