Revista Dilemas Contemporáneos: Educación, Política y Valores.
http://www.dilemascontemporaneoseducacionpoliticayvalores.com/
Año: XIII Número: 1 Artículo no.:40 Período: 1 de septiembre al 31 de diciembre del 2025

TÍTULO: Redes sociales e instituciones ante el ciberdelito: análisis de la percepción de confianza digital.

AUTORES:

1. Dr. Octavio Quintero Avila.

2. Dr. Juan Antonio Caballero Delgadillo.

RESUMEN: Este estudio analiza la percepción de confianza digital que tienen estudiantes universitarios frente a las redes sociales y las instituciones encargadas de prevenir el ciberdelito. Se aplicó una escala validada a 378 estudiantes de una universidad privada en Monterrey, Nuevo León. Los resultados muestran mayor confianza en actores cercanos como familiares y expertos en informática, y menor confianza en actores institucionales como policías y jueces. Se identificaron diferencias significativas por género, donde los hombres reportaron niveles más altos de confianza digital. Los hallazgos aportan evidencia útil para fortalecer estrategias de prevención, alfabetización digital y legitimidad institucional frente a los riesgos cibernéticos que afectan a poblaciones jóvenes altamente conectadas.

PALABRAS CLAVES: ciberdelito, ciberseguridad, criminología, instituciones, percepción.

TITLE: Social networks and institutions in the face of cybercrime: analysis of the perception of digital trust.

AUTHORS:

1. PhD. Octavio Quintero Avila.

2. PhD. Juan Antonio Caballero Delgadillo.

ABSTRACT: This study examines the perception of digital trust among university students toward social networks and the institutions responsible for preventing cybercrime. A validated scale was used with 378 students from a private university in Monterrey, Nuevo León. The results show higher trust in close actors such as family members and IT experts, and lower trust in institutional actors like police and judges. Significant gender differences were found, with male students reporting higher levels of digital trust. The findings offer useful evidence to support prevention strategies, digital literacy, and institutional legitimacy in addressing cyber risks that affect highly connected youth populations.

KEY WORDS: cybercrime, cybersecurity, criminology, institutions, perception.

INTRODUCTION.

Criminology, as a multidisciplinary science, plays a fundamental role in the comprehensive understanding of the criminal phenomenon. This discipline not only focuses on the study of antisocial behaviors, but also analyzes in an articulated manner the criminal event, the victim and the offender, also considering the social and cultural environment in which they develop (Quintero-Avila et al., 2024). In recent decades, various methodologies have been developed to observe, visualize and analyze crime, including the study of the social perception of insecurity, the use of emergency reports as a source of analysis, the application of situational prevention models in school environments, and even the profiling of cybercriminals (Quintero-Avila, 2024a, 2024b, 2025; Quintero-Avila et al., 2024, 2025; Quintero-Avila and Caballero-Delgadillo, 2024, 2025a, 2025b; Soto-Muñoz et al., 2025).

In this context, contemporary criminology is undergoing a process of transformation, adapting to the challenges posed by the digital era. Just as crime has transcended physical boundaries to manifest itself in virtual environments, it is urgent that criminological sciences expand their field of study to cyberspace, a scenario where risks are diffuse, threats are anonymous, and no person is exempt from becoming a victim. Therefore, a critical analysis of digital security and trust, as well as of the institutions in charge of its protection, is essential in an environment where permanent exposure to social networks and technological platforms poses new forms of victimization, anonymity and impunity.

Numerous recent studies have addressed cybersecurity from various perspectives, evidencing the importance of understanding how university students relate to digital risks and available protection measures. Research has explored dimensions such as attitudes toward computer security, gender differences in digital information management, and the level of knowledge young people possess regarding responsible use of technologies (Bottyan, 2023; Crabb et al., 2024; Saeed, 2023). Likewise, specific surveys have been developed that analyze basic practices such as the generation of secure passwords, the use of personal devices, Internet browsing and e-mail management in academic and personal contexts (Hong et al., 2023; Nilupú-Moreno et al., 2024).

Other studies have identified determinants that influence students' cybersafe behavior, including the type of technological infrastructure they have access to, the quality of the training programs they have received, and previous experiences with digital threats (López López et al., 2024). Similarly, the impact of university programs aimed at cybersecurity literacy has been evaluated, highlighting significant differences between trainees and graduates in terms of level of knowledge, perceived self-efficacy and incident response capability (Ahamed et al., 2024).

However, despite the wealth of empirical evidence available, a gap persists in the literature regarding the subjective perception that university students have of their own digital security, as well as the trust they place in the institutional and technological actors that regulate these environments. Understanding how they interpret risk, who they consider trustworthy and what factors shape their willingness to adopt safe behaviors is crucial to design effective strategies for prevention, training and digital governance in educational contexts.

In the contemporary digital era, the intensive use of the Internet has reconfigured the social, academic and communicational dynamics of young university students, making them a population highly exposed to the risks associated with the cyber environment. This transformation has been particularly evident in Mexico, where digital access and connectivity show sustained growth. According to the National Survey on Availability and Use of Information Technologies in Households (ENDUTIH, 2024), 97.0% of people between 18 and 24 years old, a group comprising mostly university students, are Internet users, registering an average daily use of 5.7 hours. This pattern of digital consumption significantly exceeds the national average (4.4 hours) and reveals the centrality that digital platforms have acquired in the daily routines of this population sector.

Access is predominantly through smartphones, used by 96.6% of users, which facilitates constant and ubiquitous connectivity. The most frequent activities include the use of social networks (91.5%), instant messaging services, information search, consumption of audiovisual content, and to a lesser extent, interaction with government institutions (19.1 %) or financial services digital (15.5 %) (ENDUTIH, 2024). This marked orientation towards social, informational and recreational use of the digital environment contrasts with the limited participation in institutional and digital security services, which may influence the perception of vulnerability and distrust in the face of cybercrime.

Indeed, the digital ecosystem not only expands educational, employment and entertainment opportunities, but also increases exposure to cybercrime such as fraud, identity theft, cyberbullying, profile impersonation or privacy violations. These threats, which transgress individual security, frequently operate in spaces that are highly used by university students, such as social networks and cloud services, and generate an environment in which the perception of risk is intertwined with trust or distrust towards digital platforms and the bodies that regulate them.

Digital trust, understood as users' subjective perception of the capacity, integrity and credibility of institutional and technological actors to safeguard their online security, is a critical variable for understanding behavior and attitudes towards cybercrime. Such trust can be eroded when institutional responses are perceived as ineffective, when there is a lack of transparency in the use of personal data, or when reporting mechanisms are not very accessible or reliable.

Social networks have evolved into essential digital ecosystems over the last ten years, serving as platforms for social interaction as well as for sharing academic, professional and personal data. The growing interest in how young people perceive security in these digital environments is due to their increased exposure to various forms of cybercrime due to their active use. The study by Perafán del Campo et al (2021) examines how states and public institutions deal with cybercrime and highlights the importance of citizen trust including students in prevention mechanisms. In a complementary manner, Gonzáles (2024) analyzes how young university students construct digital subjectivities and trust in online environments, as well as how they interpret risk and safety in social networks.

The target population of this study is composed of university students, who are among the most active users of digital social platforms, and due to their high exposure, frequent use, and,in many cases, lack of knowledge about cybersecurity, also among the most vulnerable to the associated risks. Digital trust is shaped by perceptions of competence and credibility; therefore, institutions must project an image of effectiveness in the face of cybercrime to strengthen user confidence.

The motivation for this study lies in the need to better understand the elements that influence young people's trust in the digital environments they use. At the scientific level, this research contributes to an emerging field of study that combines the analysis of social, technological and psychological phenomena, focusing on the connection between digital behavior, risk perception and institutional trust. At a societal level, the results may be useful for universities, cybersecurity policy makers, platform developers and educational organizations, by providing relevant information for the formulation of more effective strategies for prevention, communication and education against cybercrime.

The general objective is to analyze the perception of digital trust that university students have regarding social networks and institutions in the face of cybercrime. This objective allows establishing relationships between variables such as the level of use of social networks, exposure to cybercrime events and declared trust towards different institutional actors.

DEVELOPMENT.

Methodology.

This section describes the methodological approach adopted in the present research, detailing the study design, the criteria for selecting the population and the sample, the instruments used for measurement, the procedure followed for data collection, as well as the statistical strategies and analysis techniques used to interpret the results.

Study design.

This study used a quantitative methodology and a cross-sectional descriptive design. The main objective was to examine how university students perceive digital trust in relation to two important areas: social networks and the organizations in charge of stopping, managing and punishing cybercrime.

Population and sample.

The population under study consisted of students from a private university located in the municipality of Monterrey, Nuevo León, which served as the site for the application of the instrument. The total population consisted of N = 4,916 students enrolled at the time of data collection.

A non-probabilistic convenience sampling method was used to select the participants, considering the availability, accessibility and willingness of the students to participate in the study.

To ensure representativeness with a confidence level of 95 % (Z=1.96), an expected proportion p=0.50 and margin of error e=0, the formula for finite population was used:

$$n = \frac{N \cdot Z^2 \cdot p(1-p)}{e^2 \cdot (N-1) + Z^2 \cdot p(1-p)}$$

As a result, a final sample of n=378 students was obtained, who completed the instrument in its entirety.

Procedure and ethical considerations.

Prior to the application of the questionnaire, participants were asked for their informed consent, in which they were clearly explained the purpose of the study, the voluntary nature of their participation, as well as the guarantee of confidentiality and anonymity. It was emphasized that no names or any personal data that would allow individual identification would be collected, thus ensuring the ethical safeguarding of the information.

The survey was disseminated and answered in a controlled environment within the university's facilities, which made it possible to establish adequate conditions for application, ensuring comfort, concentration and free decision on the part of the students.

In order to guarantee the validity and relevance of the sample, the following inclusion and exclusion criteria were established.

Inclusion criterio:

- To be a student over 18 years of age.
- To be enrolled in the educational institution during the period of application of the instrument.
- To have expressly given informed consent.

Exclusion criterio:

- Being under 18 years of age or not being formally enrolled in the institution during the study period.
- Not having provided informed consent (cases with incomplete registration or without confirmation).
- Duplicate responses, detected by coincidence in the e-mail address.

Instrument.

The perception of digital trust, understood as the subjective judgment that users make about the capacity, credibility and legitimacy of various actors to protect them against cybercrime, was evaluated by means of an eight-item scale designed and validated by the University Observatory on Cybercrime. This scale was developed specifically to measure the levels of trust that university students place in different social, technological and institutional actors in the context of digital risks.

Each participant answered the items on a five-point Likert-type scale, where "1" equaled "Very little" and "5" equaled "Very much", assessing their level of trust in relation to the following scenarios or sources of protection: traditional media, social networks, law enforcement officials, judicial officials, family or friends in cybersecurity issues, and computer experts.

The reliability of the scale was assessed using Cronbach's alpha coefficient, obtaining a value of $\alpha = .993$, indicating excellent internal consistency

Data collection and processing.

Data collection was carried out using the Microsoft Forms digital platform, where the questionnaire designed to measure the perception of digital trust in the face of cybercrime was hosted. The application of the instrument was carried out during a continuous period of 73 days, in coordination with school authorities and teachers. The questionnaire was completed in a controlled environment within the university facilities, with an average response time of 7 minutes and 29 seconds.

Once the survey phase was completed, the data were exported in CSV format and processed using Jamovi Desktop software, version 2.6.44 for macOS. Prior to statistical analysis, the database was thoroughly cleaned. This stage included the identification and elimination of incomplete records, unfinished surveys, as well as duplicate responses detected by matching e-mail addresses.

Likewise, cases that did not meet the inclusion criteria, such as participants who were minors or not enrolled in the corresponding period, were discarded. After applying these filters, only the set of valid responses that met the previously established ethical, methodological and technical criteria was retained, which ensured the quality and consistency of the information analyzed.

Results.

This section presents the findings derived from the statistical analysis applied to the database constructed from the valid questionnaires (n = 378). The results are organized according to the different types of analysis carried out to explore patterns of digital trust towards social and institutional actors. This evidence allows us to identify the levels of trust perceived by university students in the face of cybercrime, differentiating between public actors (such as police or judges) and private actors (such as social networks or computer experts).

Table 1 presents the descriptive statistics corresponding to each of the items that make up the scale, representing different social and institutional actors before which the participants evaluated their level of trust in the face of cybercrime.

Table 1. Descriptive statistics by source of trust in cybercrime.

	Traditional media	**Social networks**	**Police officers**	**Judicial officials**	**Family/friends on cybersecurity issues**	**Computer experts**
N	378	378	378	378	378	378
Average	3.34	3.20	3.10	3.12	3.47	3.44
Median	3.00	3.00	2.00	3.00	3.00	3.00
Standard deviation	1.46	1.44	1.52	1.52	1.35	1.33
Minimum	1	1	1	1	1	1
Maximum	5	5	5	5	5	5

The results show that the sources in which students place the highest level of trust are family and friends on cybersecurity issues (M = 3.47, SD = 1.35), followed by computer experts (M = 3.44, SD = 1.33) and traditional media (M = 3.34, SD = 1.46). In contrast, the lowest levels of trust were observed in police officers (M = 3.10, SD = 1.52) and judicial officers (M = 3.12, SD = 1.52), suggesting a more critical institutional perception on the part of the participants.

Figure 1 shows the density distribution of the perception of digital trust that university students assigned to six social and institutional actors. The results reveal polarized response patterns for most of the actors evaluated, with noticeable concentrations at the extremes of the scale. In the case of traditional media (a), a clear bimodality is observed, with outstanding densities in values 2 and 5, reflecting a perception divided between distrust and high trust. Social networks (b) present a similar distribution, showing ambivalent positions possibly influenced by constant exposure to contradictory information and diverse personal experiences. For police (c) and judicial (d) officials, the predominant concentration is located at value 2, with a second peak at value 5, indicating that a large segment of the sample expresses institutional distrust, although there is another group that grants full trust to these actors, reaffirming the polarization around the state apparatus. In contrast, family members and friends in cybersecurity issues (e) show a more balanced distribution, with greater density in values 3 and 5, suggesting a more homogeneous perception of trust towards figures in the close environment.

Finally, computer experts (f) stand out for a concentration in the higher levels (4 and 5), which positions them as the actors with the highest level of perceived trust in the digital environment. Overall, these findings suggest that digital trust among university students tends to be oriented more towards technical or personal referents, while public institutions face a more fragmented and skeptical perception scenario regarding their protective role in the face of cybercrime.

Figure 1. Density distribution by actor of trust in the face of cybercrime.

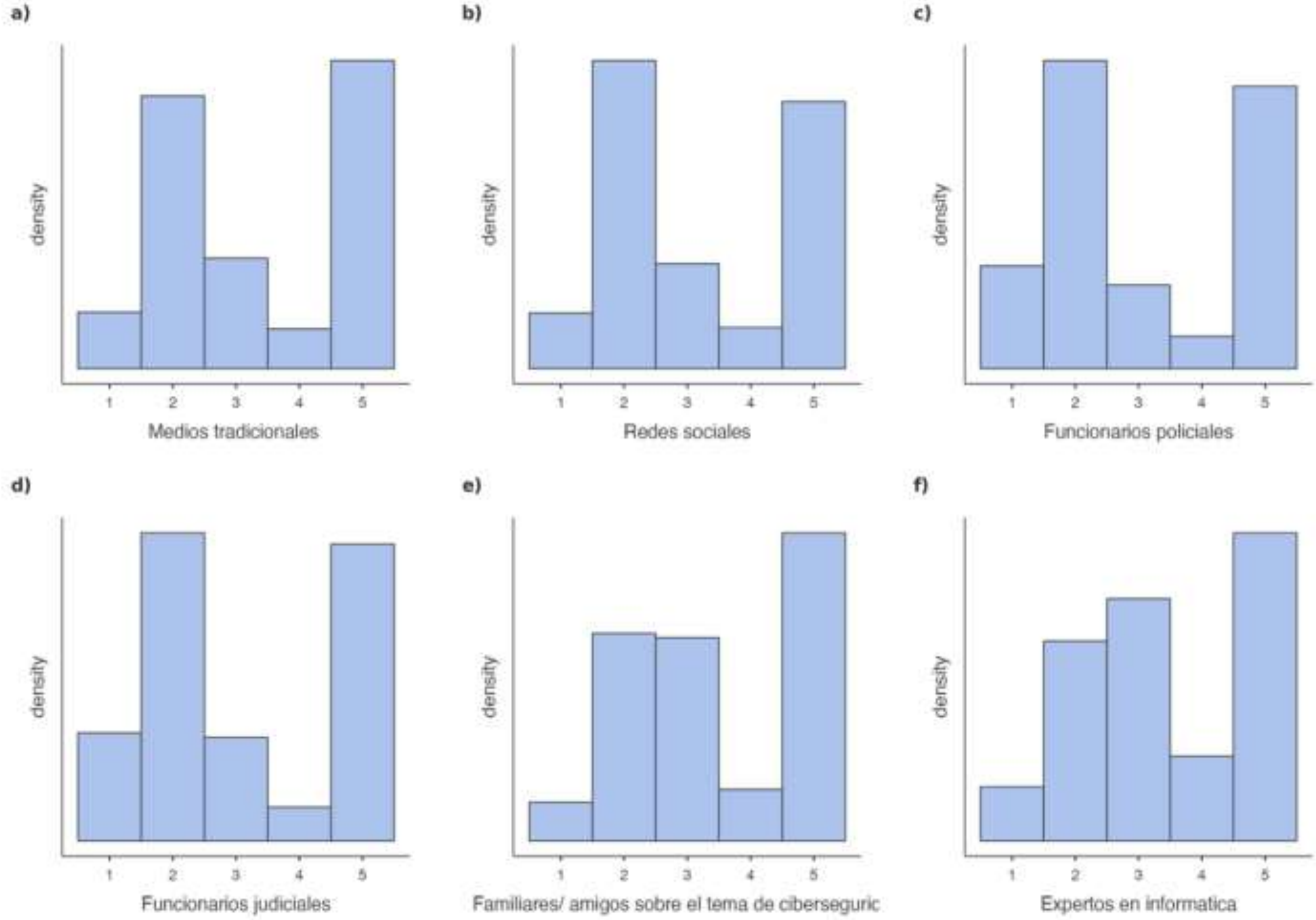
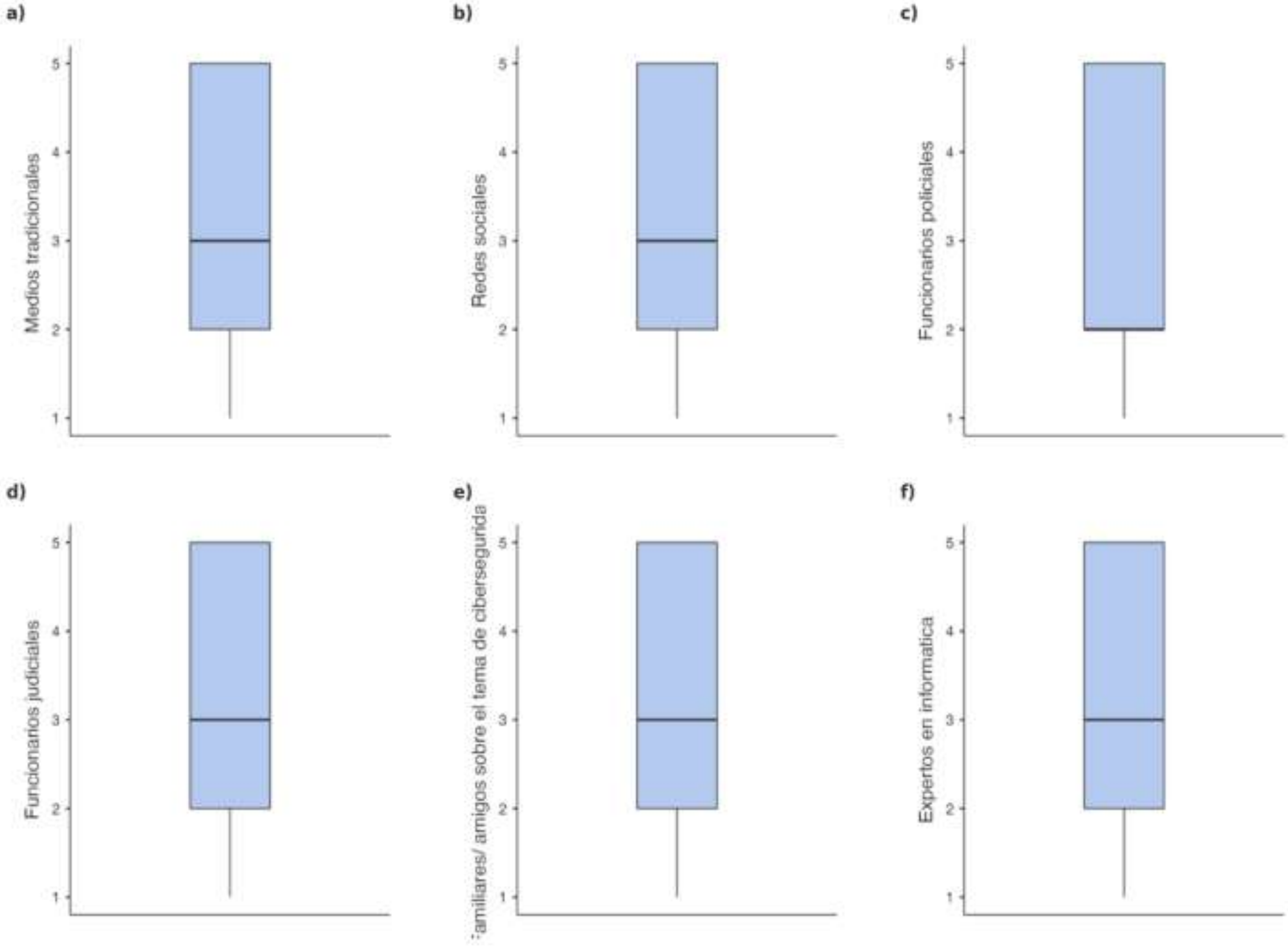


Figure 2 presents boxplots for each of the six actors assessed on the digital trust perception scale. These graphs allow us to visualize the distribution of the data, the dispersion of the responses, the positions of the medians and possible asymmetries in the participants' evaluations.

In the case of traditional media (a), the median is at value 3, with an interquartile range that spans from low values to the maximum level (5), confirming a wide and dispersed distribution. Social networks (b) show a similar median (3), but with lower lower dispersion, indicating a slight tendency towards moderate trust. Police officers (c) show a median value of 2, the lowest of all the actors evaluated, reflecting a generalized tendency towards distrust, with a distribution more skewed towards lower values. Similarly, judicial officials (d) show a median of 3, although with a notable lower range, evidencing the existence of responses with low institutional trust. On the other hand, family members or friends in cybersecurity issues (e) show a median of 3, but with a higher density towards higher values, indicating a more positive and homogeneous perception. Finally, computer experts (f) also exhibit a median at 3, but with a narrower and more centered box, suggesting a concentration of responses at medium-high levels of trust. Overall, the box plots reinforce the reading that university students present a greater dispersion and tendency to distrust institutional actors (police and judicial officials), while close or specialized actors, such as family members or computer experts, tend to concentrate on higher levels of perceived trust.

Figure 2. Boxplots of the perception of digital trust.



Note. Likert-type scale from 1 = Very little to 5 = Very much.

The results of Table 2 obtained through the t-test for independent samples showed statistically significant differences in all the actors evaluated in the digital trust perception scale between male and female students. In all cases, the p-value was less than .001, which allows rejecting the null hypothesis of equality of means and suggests that gender has a relevant effect on the levels of trust assigned to different social and institutional actors linked to cybercrime. The data show that women reported significantly higher levels of trust than men in all items of the scale.

The most pronounced differences were observed in trust toward police officers (t = -48.0, gl = 376, p < .001, d = -5.01), social networks (t = -47.9, p < .001, d = -5.00) and judicial officials (t = -46.0, p < .001, d = -4.81). Significant differences were also identified in perceptions toward traditional media (t = -46.6, p < .001, d = -4.86), family or friends on cybersecurity issues (t = -41.1, p < .001, d = -4.29), and computer experts (t = -37.1, p < .001, d = -3.87).

It is noteworthy that the effect sizes, measured by Cohen's d, were extremely high in all cases, exceeding absolute values of 3.80. This not only indicates robust statistical significance, but also remarkable practical relevance. The findings reinforce the hypothesis that gender strongly influences the construction of digital trust. Specifically, the observed pattern suggests that women tend to express greater trust in all the evaluated actors, which could be associated with a greater perception of digital vulnerability, greater awareness of cyber risks or a proactive attitude in seeking protection within digital environments.

Table 2. Differences in perception of digital trust according to gender.

<table>
<tr><th colspan="7">t-test for Independent Samples</th></tr>
<tr><th></th><th></th><th>Statistic</th><th>gl</th><th>p</th><th></th><th>Effect Size</th></tr>
<tr><td>Traditional means</td><td>Student's t</td><td>-46.6[a]</td><td>376</td><td><.001</td><td>Cohen's d</td><td>-4.86</td></tr>
<tr><td>Social networks</td><td>Student's t</td><td>-47.9</td><td>376</td><td><.001</td><td>Cohen's d</td><td>-5.00</td></tr>
</table>

t-test for Independent Samples						
		Statistic	**gl**	**p**		**Effect Size**
Police officers	Student's t	-48.0	376	<.001	Cohen's d	-5.01
Judicial officers	Student's t	-46.0	376	<.001	Cohen's d	-4.81
Family/friends on the topic of cybersecurity.	Student's t	-41.1[a]	376	<.001	Cohen's d	-4.29
Computer experts	Student's t	-37.1[a]	376	<.001	Cohen's d	-3.87

Table 3 presents the descriptive statistics of the perception of digital trust, differentiated by gender, for each of the actors evaluated. The results show substantial and consistent differences between female and male students, with males reporting significantly higher levels of trust in all social and institutional actors related to cybersecurity.

In relation to traditional media, females scored a mean of 2.21 (SD = 0.708), while males achieved a mean of 4.94 (SD = 0.233), representing a significant gap of more than two points on the Likert scale. This trend is repeated with social networks, where women recorded a mean of 2.08 (SD = 0.563) versus 4.78 (SD = 0.510) for men. Police officers also showed a clear difference: mean of 1.91 (SD = 0.585) in the female group versus 4.78 (SD = 0.550) in the male group. A similar situation was observed with judicial officials, with means of 1.95 and 4.78, respectively.

Regarding non-institutional actors, such as family members or friends on cybersecurity issues, women showed a mean of 2.45 (SD = 0.716), while men reached 4.92 (SD = 0.276). Finally, with respect to computer experts, the pattern remained the same, with a mean of 2.45 (SD = 0.741) for women and 4.83 (SD = 0.373) for men.

These differences are also reflected in the medians, being 2.00 for all categories in the female group, while in the male group the median was 5.00 in all cases, except for computer experts, where it was 5.00 in both groups but with greater dispersion in females. Overall, the descriptive data evidences a clear disparity in the construction of digital trust between both genders, suggesting that the male perception is marked by a significantly higher trust towards all the evaluated actors. These differences become more relevant when considered in conjunction with previously reported inferential results, which demonstrated statistically significant differences with large effect sizes.

Table 3. Descriptives by gender in the perception of digital confidence.

Group Descriptives						
	Group	**N**	**Mean**	**Median**	**SD**	**EE**
Traditional means	Female	221	2.21	2.00	0.708	0.0477
	Male	157	4.94	5.00	0.233	0.0186
Social networks	Female	221	2.08	2.00	0.563	0.0379
	Male	157	4.78	5.00	0.510	0.0407
Police officers	Female	221	1.91	2.00	0.585	0.0394
	Male	157	4.78	5.00	0.550	0.0439
Judicial officers	Female	221	1.95	2.00	0.616	0.0414
	Male	157	4.78	5.00	0.550	0.0439
Family/friends on cybersecurity issue	Female	221	2.45	2.00	0.716	0.0481
	Male	157	4.92	5.00	0.276	0.0221
Computer experts	Female	221	2.45	3.00	0.741	0.0498

Group Descriptives						
	Group	**N**	**Mean**	**Median**	**SD**	**EE**
	Male	157	4.83	5.00	0.373	0.0298

Figure 3 presents the comparison of means between men and women for each of the six actors evaluated in the digital trust perception scale, showing the mean values with their respective 95% confidence intervals. The subgraphs (a-f) correspond to the items:

(a) Traditional media.

(b) Social networks.

(c) Police officers.

(d) Judicial officers.

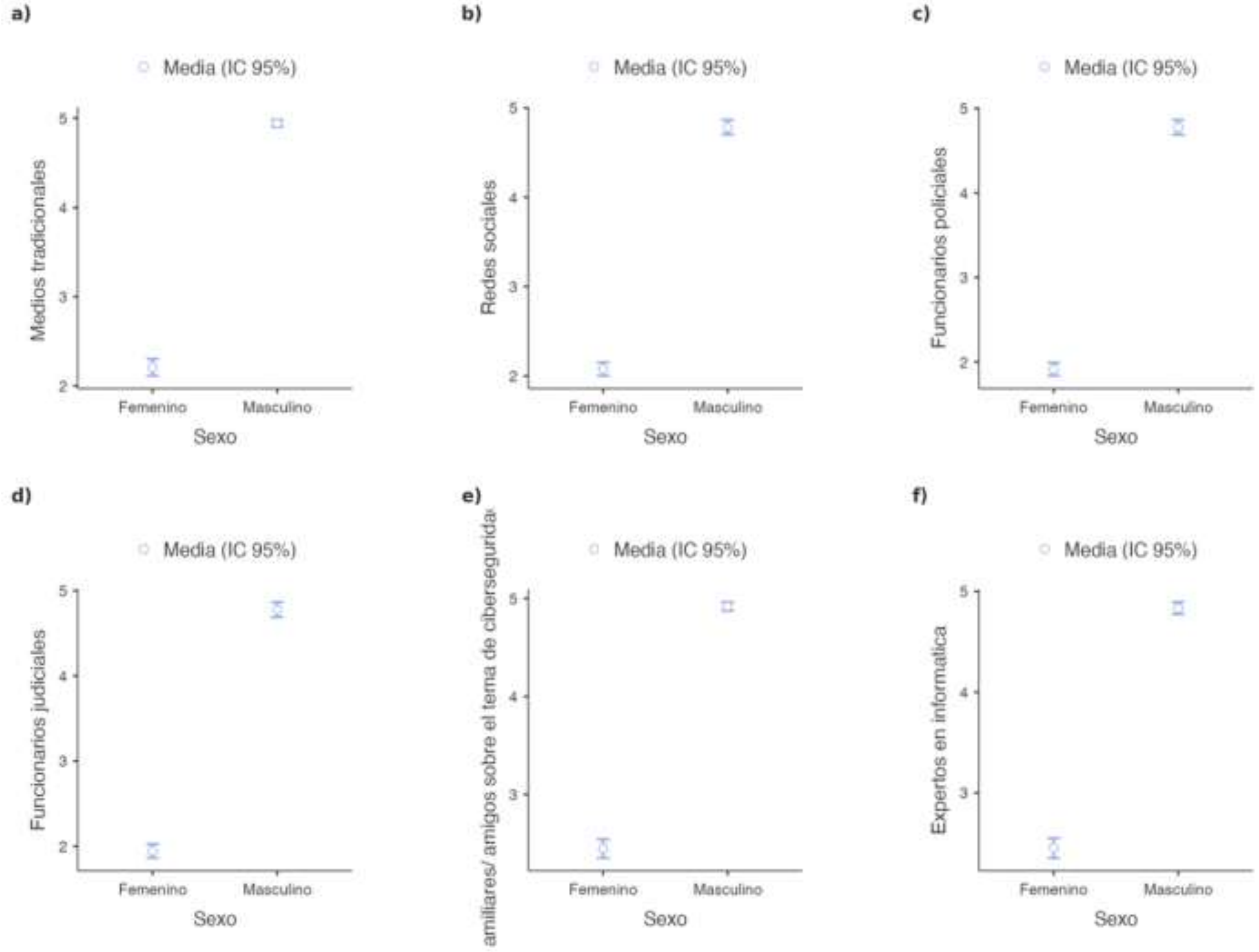
(e) Family/friends in cybersecurity issues.

(f) Computer experts.

The results visually and powerfully show a consistent trend: male participants report significantly higher levels of trust than female participants in all the actors evaluated. Not only are the observed differences wide, but the confidence intervals of the two groups do not overlap, reinforcing the statistical significance previously identified through Student's t-tests.

In practical terms, male students reported greater trust in both formal institutions (police, justice) and informal or social settings (media, networks, friendships and technical experts). This trend suggests a differentiated construction of digital trust according to gender, which could be mediated by factors such as perception of vulnerability, previous experiences of digital victimization or differential socialization regarding the use of technologies and information channels.

Figure 3. Confidence intervals (95%) in perception of digital trust according to gender.



CONCLUSIONS.

The present study made it possible to analyze, from an empirical and quantitative perspective, the levels of digital trust shown by university students towards various social and institutional actors in the context of cybercrime. The results show that, although there is a moderate trust towards technical and close environment figures such as computer experts and family or friends in cybersecurity issues, a more critical and polarized perception towards formal institutions, especially towards police and judicial officials was identified.

Specifically, the general objective of this research was met: to analyze the perception of digital trust that university students have towards social networks and institutions in the face of cybercrime. From the findings obtained, it was possible to establish relationships between key variables such as the type of actor evaluated, institutional membership, gender of the participant, and the declared level of trust, thus providing useful empirical evidence to understand how trust in digital environments is configured by a young university population.

Likewise, statistically significant differences were corroborated according to the gender of the participants. Male students showed significantly higher levels of digital trust compared to their female counterparts, both in media and social networks and in institutions of the penal system. These differences were consistent in Student's t-tests, descriptive analyses, and plotted confidence intervals, with extraordinarily high effect sizes. This finding suggests a differentiated construction of digital trust based on gender, possibly linked to factors such as risk perception, previous experience with digital incidents, and individual strategies for protection against cybercrime.

From a criminological perspective, the results reinforce the need to rethink prevention strategies and institutional digital communication. Mistrust of public actors, in an environment where digital victimization is growing and becoming increasingly sophisticated, represents a major barrier to the effectiveness of cybersecurity policies. Therefore, there is a need to strengthen institutional credibility, as well as to expand training digital specifically aimed at the most vulnerable sectors, such as young women who are intensive users of technological platforms.

In methodological terms, the reliability of the scale applied ($\alpha = .993$) and the data cleaning provide robustness to the results obtained. However, future research could incorporate qualitative analyses to understand in greater depth the social imaginaries that shape digital trust, as well as extend the study to other population sectors and university, public and private contexts.

This study provides key evidence for the design of interventions aimed at improving digital security and rebuilding institutional legitimacy in the virtual environment, with emphasis on a criminology adapted to the challenges of the 21st century.

BIBLIOGRAPHICAL REFERENCES.

1. Ahamed, Bulbul, Polas, Mohammad Rashed Hasan, Kabir, Ahmed Imran, Sohel-Uz-Zaman, Abu Saleh Md., Fahad, A. Al, Chowdhury, Saima, & Rani Dey, Mrittika. (2024). Empowering Students for Cybersecurity Awareness Management in the Emerging Digital Era: The Role of Cybersecurity Attitude in the 4.0 Industrial Revolution Era. SAGE Open, 14(1), 21582440241228920. https://doi.org/10.1177/21582440241228920
2. Bottyan, L. (2023). Cybersecurity awareness among university students. Journal of Applied Technical and Educational Sciences, 13(3), ArtNo: 363. https://doi.org/10.24368/jates363
3. Crabb, J., Hundhausen, C., & Gebremedhin, A. (2024). A Critical Review of Cybersecurity Education in the United States. Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. 1, 241–247. https://doi.org/10.1145/3626252.3630757
4. Gonzáles, M. A. (2024). Pensar las diversidades de jóvenes estudiantes en mundos posmodernos digitales. Areté, Revista Digital del Doctorado en Educación de la Universidad Central de Venezuela, 10(20). https://doi.org/10.55560/arete.2024.20.10.11
5. Hong, W. C. H., Chi, C., Liu, J., Zhang, Y., Lei, V. N.-L., & Xu, X. (2023). The influence of social education level on cybersecurity awareness and behaviour: a comparative study of university students and working graduates. Education and Information Technologies, 28(1), 439–470. https://doi.org/10.1007/s10639-022-11121-5
6. Instituto Nacional de Estadística y Geografía. (2024). ENDUTIH 2024 Principales Resultados. https://www.inegi.org.mx/programas/endutih/2024/#documentacion

7. López López, H. L., Quirino Rodríguez, L. G., & Carrasco Valenzuela, A. C. (2024). Percepción de la ciberseguridad entre estudiantes universitarios en entornos digitales: Un estudio en la Facultad de Informática Mazatlán. TIES, Revista de Tecnología e Innovación en Educación Superior, 11, 72–95. https://doi.org/10.22201/dgtic.26832968e.2024.11.30

8. Nilupú-Moreno, K., Salas-Riega, J. L., Ninaquispe-Soto, M., & Riega-Virú, Y. (2024). Cybersecurity in University Students: A Systematic Review of the Literature. En A. K. Nagar, D. S. Jat, D. K. Mishra, & A. Joshi (Eds.), Intelligent Sustainable Systems (pp. 315–332). Springer Nature Singapore.

9. Perafán Del Campo, E. A., Polo Alvis, S., Sánchez Acevedo, M. E., & Miranda Aguirre, C. (2021). Estado y soberanía en el ciberespacio. Via Inveniendi Et Iudicandi, 16, 1–46. https://www.redalyc.org/articulo.oa?id=560268690006

10. Quintero Avila, O., Garcia Herrera, D. G., & Caballero Delgadillo, J. A. (2025). Cybercriminologia e profilo del cybercriminale. En la ricostruzione criminologica dell'evento (Vol. 1, Número 1, pp. 288–310). Diritto Più.

11. Quintero-Avila, Hernández-Valdez, & Soto-Muñoz. (2025). Análisis geoespacial de la percepción de inseguridad en el campus Ciudad Universitaria de San Nicolás de los Garza, Nuevo León. Ciencia UANL, 28(133), 39–43.

12. Quintero-Avila, O. (2024a). El Análisis y mapeo delictivo para el desarrollo de políticas públicas de seguridad en México. Constructos Criminológicos, 4(7), 159–170. https://doi.org/10.29105/cc4.7-86

13. Quintero-Avila, O. (2024b). Un análisis de la percepción de seguridad durante la pandemia de COVID-19 en la colonia México Lindo en San Nicolás de los Garza, Nuevo León, México. Estudios de la Seguridad Ciudadana, 9(7), 149–178. https://revista.ucs.edu.mx/wp-content/uploads/2024/08/Art-7-Vol-9.pdf

14. Quintero-Avila, O. (2025). Análisis espacial del delito: violencia de género en Monterrey, Nuevo León. En Mario Alberto Garza Catillo, Octavio Quintero Avila, & Juan Antonio Caballero Delgadillo (Eds.), Perspectivas criminológicas. En la inteligencia criminal estratégica (1a ed., Vol. 1, Número 1, pp. 63–104). Tirant Humanidades. http://eprints.uanl.mx/29410/7/29410.pdf

15. Quintero-Avila, O., & Caballero-Delgadillo, J. A. (2024). Análisis Espacial de la Violencia de Género contra la Mujer: Estudio de Reportes de emergencias 911 mediante Sistemas de Información Geográfica. Revista Veritas Et Scientia-UPT, 13(2), 179–193. https://doi.org/10.47796/ves.v13i2.1111

16. Quintero-Avila, O., & Caballero-Delgadillo, J. A. (2025a). El análisis delictivo como herramienta en la construcción de estrategias de prevención social y delincuencial. Constructos Criminológicos, 5(8), 55–74. https://doi.org/10.29105/cc5.8-101

17. Quintero-Avila, O., & Caballero-Delgadillo, J. A. (2025b). Percepción de Inseguridad Urbana: Enfoque Geoespacial para el análisis criminológico. Dilemas contemporáneos: Educación, Política y Valores, 12(3), 1–25. https://doi.org/10.46377/dilemas.v12i3.4692

18. Quintero-Avila, O., Caballero-Delgadillo, J. A., & García-Herrera, D. G. (2025). Visualización de la inseguridad. Divulgación de Ciencia y Educación, 2(3), 38–40. https://redicye.upeg.edu.mx/2025/01/22/visualizacion-de-la-inseguridad/

19. Quintero-Avila, O., Caballero-Delgadillo, J. A., Hernández-Valdez, O. A., MÁ., S.-M., & García-Herrera, D. G. (2024). Estrategias metodológicas para el análisis y mapeo delictivo en las ciencias sociales. Perspectivas, 9(24), 257–280. https://doi.org/10.26620/uniminuto.perspectivas.9.24.2024.257-280

20. Quintero-Avila O, & Caballero-Delgadillo JA. (2025). Perspectivas criminológicas En la inteligencia criminal estratégica (Tirant Humanidades, Ed.; 1a ed., Vol. 1). Tirant Humanidades.

21. Saeed, S. (2023). Education, Online Presence and Cybersecurity Implications: A Study of Information Security Practices of Computing Students in Saudi Arabia. Sustainability, 15(12). https://doi.org/10.3390/su15129426

22. Soto-Muñoz, M. Á., Quintero-Avila, O., & Caballero-Delgadillo, J. A. (2025). Prevención situacional del delito: Percepción de menores sobre riesgos en su entorno escolar. Estudios de la seguridad ciudadana, 11(8), 47–68.

AUTHORS' DATA.

1. **Octavio Quintero Avila.** Doctor in Criminology. Professor at the Universidad Autónoma de Nuevo León, México. E-mail: Octavioquinteroavila@gmail.com

2. **Juan Antonio Caballero Delgadillo** Doctor in Criminology. Professor at the Universidad Autónoma de Nuevo León, México. E-mail: alfacoca123@gmail.com

RECIBIDO: 28 de mayo del 2025. **APROBADO:** 6 de junio del 2025.