Article **ECORFAN Journal-Republic of Colombia**
December, 2022 Vol.8 No.15 1-14

Social and university networks. Study on the perception of privacy and its management

Redes sociales y universitarias. Estudio sobre la percepción de la privacidad y su gestión

GARIZURIETA-BERNABE, Jessica†*, GONZÁLEZ-BENÍTEZ, Rubén Álvaro, MORALES-TOXQUI, Jazmin and RAMÍREZ-SÁNCHEZ, Jesús

Universidad Veracruzana, Facultad de Contaduría y Administración.

ID 1st Author: *Jessica, Garizurieta-Bernabe* / **ORC ID:** 0000-0002-1443-4737, **CVU CONACYT ID:** 273881

ID 1st Co-author: *Rubén Álvaro, Gonzlález-Benítez* / **ORC ID:** 0000-0002-6396-0100

ID 2nd Co-author: *Jazmin, Morales-Toxqui* / **ORC ID:** 0000-0001-5071-6013

ID 3rd Co-author: *Jesús, Ramírez-Sánchez* / **ORC ID:** 0000-0003-4673-3480

DOI: 10.35429/EJC.2022.15.8.1.14 Received September 08, 2022; Accepted December 30, 2022

Abstract

Virtual social networks have established themselves as the tool for greater communication between young university students. Through them, they allow the exchange of information, in addition to sharing experiences and creating social relationships quickly. This article determines indices of factors to explain the use of social networks in students; On the other hand, there are bad practices in the use of these, exposing personal information. Some of the main dangers in social networks are identity theft, spam, cyberbullying, defamation, sexting and sextortion, to name a few. The objective of the current work is to analyze the use of social networks by university students, since this can be explained by the factors of integrity, ease of use, attitude, and intention. Likewise, it is directly related to the satisfaction of the needs of inclusion, belonging and social recognition. The study was carried out in the population of four programs belonging to the Universidad Veracruzana (UV), specifically the Faculty of Accounting and Administration (FCA), and although the four programs can be considered as digital natives, the data expose that they require education in terms of digital literacy. It also analyzes how to manage these social networks and know how informed they are about: the privacy notices that social networks handle, with whom they expose personal information and what happens to the information they publish, also, knowledge regarding security measures in social networks

Social media, University students, Social risks

Resumen

Las redes sociales virtuales se han consolidado como la herramienta de mayor comunicación entre jóvenes universitarios, a través de ellas, permiten intercambio de información, además de compartir experiencias y de crear relaciones sociales de forma rápida. Este articulo determina índices de factores para explicar el uso de las redes sociales en estudiantes; por otro lado, existen malas prácticas en el uso de estas, dejando al descubierto información personal. Algunos de los principales peligros en las redes sociales se encuentran: el robo de identidad, spam, ciberacoso, difamación, ciberbyllying, sexting y sextorsión, por mencionar algunos. El objetivo del actual trabajo es analizar el uso de las redes sociales por parte de los universitarios, ya que este se puede explicar mediante los factores de integridad, facilidad de uso, actitud e intención; así mismo, está directamente relacionado con la satisfacción de las necesidades de inclusión, pertenencia y reconocimiento social. El estudio se realizó, en la población de cuatro programas pertenecientes a la Universidad Veracruzana (UV), específicamente de la Facultad de Contaduría y Administración (FCA), y aunque los cuatro programas pueden ser considerados como nativos digitales, los datos exponen que requieren educación en términos de alfabetización digital. También se analiza la forma de gestionar estas redes sociales y conocer que tan informados están respecto a: los avisos de privacidad que manejan las redes sociales, con quién exponen la información personal y qué sucede con la información que publican, asimismo, el conocimiento en cuanto a medidas de seguridad en las redes sociales.

Medios sociales, Estudiantes universitarios, Riesgos sociales

Citation: GARIZURIETA-BERNABE, Jessica, GONZÁLEZ-BENÍTEZ, Rubén Álvaro, MORALES-TOXQUI, Jazmin and RAMÍREZ-SÁNCHEZ, Jesús. Social and university networks. Study on the perception of privacy and its management. ECORFAN Journal-Republic of Colombia. 2022. 8-14: 1-14

* Correspondence to Author (e-mail: jgarizurieta@uv.mx)
† Researcher contributing as first author.

1. Introduction

In recent decades, Information and Communication Technologies (ICT, hereinafter) have generated changes and innovations (Jasso, López, & Díaz, 2017). They have spread in almost all aspects of daily activities (Del Barrio & Ruíz, 2016), which has constituted an unprecedented transformation at a dizzying pace and with an uncertain direction (Jordán, Galperin, & Peres, 2010).

Among the most important technological innovation tools are virtual social networks (Castro & Moral, 2017), which have produced new forms of communication and interaction between people (Osorio, Molero, Pérez, & Mercader, 2016). Established as a technology of almost universal character, they exert great influence on people of all ages (Osorio *et al*., 2016), especially on young people (García & Nazaret, 2017; Jasso *et al*., 2017), located in the university environment (Domínguez & López, 2015; Garcia, Seco, & Del Hoyo, 2013; Gómez, Roses, & Farias, 2012; Martinez, 2018).

According to Usla (2020), the most widely used virtual social networks are: Google, Instagram, Twitter, Facebook, WhatsApp and YouTube; being the last three applications the fastest growing during the health contingency. The research aims to determine indices of factors that explain the use of social networks. In recent years, the perspective of security has been analyzed, as a phenomenon directly linked to social networks, because they have become indispensable in the family, school and work environment; leading to an overexposure of users. The article is divided into five sections: the first makes an approach to virtual social networks; the second describes the theoretical approach; the third sets out the materials and methods; The fourth shows the main results and the fifth presents the conclusions.

2. Social Networks

Virtual social networks are the result of "interpersonal and group communication maintained by a series of individuals over time" (García *et al*., 2013, p. 96), and therefore meet the criteria of the classic term communication and its postulates, but when including the technological object (Arab & Díaz, 2015), virtuality must be taken into consideration.

Therefore, the word virtual social networks can be defined as "a set of actors (or nodes) that are united by the social relations established between them" (Casaló, Flavián, & Guinalíu, 2012, p. 43). The concept of social network, under the approach addressed in this research, has particular qualities and structure. One of the main considerations that must be taken into account is that a social network is shared at the community level and allows remote communication between a set of autonomous teams connected by technical means (Gordona, n.d.). Santos (1989) distinguishes four elements in social networks:

– Network location. Which is determined by some specific actor that refers to the point where it is anchored (for example, the website).

– Accessibility. Which is defined by the number of steps needed to reach another actor to define its magnitude, the proportion of actors that can contact each actor in the network and the number of intermediaries that must be used to connect with another must be considered.

– Density. It refers to the number of links that must be crossed to reach an actor, it will be greater or lesser due to the connections, that is, if some actors are linked with others, but not with all.

– Rank. It is defined as the number of people who are directly linked, without any intermediary.

Currently social networks are part of our interpersonal relationships, most people can not be without communication or even without the use of cell phones, we talk about family, school and work that is why the use of social networks has become indispensable for the human being. Among the social networks with the greatest impact are:

– Facebook. It is one of the most complete networks, since it has functions to be able to interact with new and familiar people, get informed, create business, make interactions with customers or brands in an easy and immediate way.

ISSN-On line: 2539-1372

– Instagram. It is a social network used mainly to upload photos and videos instantly, however, like Facebook it allows you to create online stores and interact with customers.

– Twitter. Virtual communication space where you can express a thought, idea or information in a summarized way, through brief messages.

– WhatsApp. Instant messaging application, allows you to send and receive a variety of types of multimedia files, such as text, photos, videos, documents and location, in addition to being able to make calls and video calls, freely, simply with the use of data or WIFI network.

Based on the above, it is possible to affirm that virtual social networks have been positioning themselves as an ideal space to socialize, share ideas and different sources of information (Caldevilla, 2010; Sánchez & Mestre, 2016), for training and entertainment (Jasso *et al*., 2017), as well as exchanging information and knowledge in a fast, simple and comfortable way (Gómez *et al*., 2012).

Given the constant evolution of virtual social networks, their classification is complex and there is no consensus. This is because they have been acquiring features, tasks and options that can include them in more than one category of those that have been proposed so far (Martínez, 2018). For analysis purposes, four types can be identified:

The first category group them into professionals, generalists and specialists (Celaya, 2000). The second category in generalists or leisure and professionals (INTECO-AEPD, 2009). The third category distinguishes between user-centric and content-centric, where what matters is the material that is shared (Aced, 2010). The fourth categorizes by theme, activity and shared content (Ponce, 2012).

The set of opportunities they offer has favored their diffusion in different sectors. Likewise, it is important to indicate that the use of these technological tools "has also spread from the lowering of costs, the use of cell phones and the viral effect of Twitter and Facebook platforms on a global scale" (Sandoval, Romero, & Heredia, 2013, p.1), becoming with the passing of the years a fundamental element (Gómez *et al*., 2012), in classrooms that concentrate digital natives (Buxarrais, 2016; Gómez *et al*., 2012; Prensky, 2001).

3. Risks and vulnerabilities in social networks

The vulnerability, in terms of computing, is a weakness or failure in an information system that puts information security at risk and may allow an attacker to compromise the integrity, availability or confidentiality of this. (INCIBE, 2017).

Currently social networks are part of our interpersonal relationships, most people can´t be without communication or even without the use of cell phones. We talk about family, school, and work that is why the use of social networks has become indispensable for the human being. Although, its use can be beneficial, you are also exposed to different risks through them. For Forbes (2014) and UNAM (2009), the worst threats on social networks are:

a) Social network viruses: These are carried out through botnets or computer robots, in this way hackers take control of computers by sending them spam emails that clicking on the link could cause damage.

b) Phishing bait: It is about hacking passwords through the e-mail that leads the user to enter the account of the social network.

c) Defamation: Users usually share information about projects, companies, and sensitive information on networks; which is infiltrated generating various scandals.

d) Trojans: Calculates the value of the victim's account through the URL zone.

ISSN-On line: 2539-1372

e) Abbreviation of links: Services that provide help to abbreviate links to fit in smaller places, hide the malware link allowing victims not to realize that they are clicking to urge it.

f) Botnets: They are used to direct and control the channels of some botnets.

g) Advanced Persistent Threats (ATP): Collects data from high-level people for whom social media can be an important source of information.

h) Cross-linking of web pages for solicitation forgery (CSRF): The moment a user shares an image in a sequence of events, other users can click to spread it.

i) Identity theft: They are those who pretend to be another person, and ascend to more users than the true profile.

j) Harassment: such as sexting (sending sexual, erotic or pornographic content), Grooming (messages from an adult with a minor in order to gain trust and thus be able to talk about sex, get sexual content and finally get a meeting to be able to abuse it), Cyberbullying (harassment or threat to a person through social networks through texts, images or videos).

The latter, and according to Barranco (2014), within cyberbullying are framed:

– Electronic insult: It is the exchange of words between two or more people through some technological device privately or in some public place.

– Harassment: An act that involves different behaviors, words, or frequent actions against a person in order to emotionally alter them. It can be carried out physically or through messages on social networks.

– Denigration: It consists of sending false information about someone and uploading it to a social network, it can be written information, photographs or videos.

– Impersonation: The harasser impersonates another person by posing access codes of the harassed person, using their account or identity with the aim of offending, malice or sending false information

Some methods of manipulation are based on the trust of the user, through which it leads to deception, such as phishing, which is increasingly adapted to social networks because it is a more persuasive environment for users and where they tend to trust so much in what they publish, as in what their friends send them without really knowing if it is true information or a reliable file (Olmo, 2017).

Although, the care of information on social networks depends on users, one of the main reasons why users do not protect their privacy is probably because they are not sufficiently aware of the data they disclose on the social network such as "the connection time, the IP address you use, your geographical location, the profiles visited, the messages received and sent" (Cragno, *et al*., 2018, p. 2), and therefore, they are not responsible for the value of your information.

In this sense, knowing the conditions on the perception and experience that university students have had in terms of security of personal data information in social networks, is preponderant, to analyze the importance that students themselves contribute to this issue.

4. Theoretical approach

To approach understanding the determinants of acceptance and use of new technologies, various theoretical models have been used (Sternad & Bobek, 2013), which suggests a lack of consensus on which are the ones that best explain the adoption processes (Jones, Motta, & Alderete, 2016; Sternad & Bobek, 2013).

The Technology Acceptance Model (TAM) developed by Davis (1989), is the first and main theory of traditional adoption in the field of Information Technology (Awa *et al*., 2015; Gangwar *et al*., 2015). Therefore, the usefulness of TAM for the purposes of the study is pertinent (Lorenzo, Gómez, & Alarcón, 2011; Shin, 2008; Willis, 2008).

ISSN-On line: 2539-1372

TAM is an extension of the Theory of Reasoned Action (TRA) developed by Ajzen & Fishbein (1975), to describe behavior towards information technologies (Blas, Mafé, & Manzano, 2008). Also of new technologies (Rodríguez & Herrero, 2008). It has been validated in a wide range of research in different applications (Ben, 2016), among which are virtual social networks (Lorenzo *et al*., 2011; Romero, De Amo, & Borja, 2011).

The model assumes that beliefs, i.e., perceived utility (UP, hereinafter) and perceived ease of use (FUP, hereinafter), influence the attitude of use (AU, onwards), which in turn leads the intention to use (IU, hereinafter) and then generates a behavior to use an Information System. Therefore, UP and FUP are the basic determinants of the acceptance of Information Systems (Davis, Bagozzi, & Warshaw, 1989).

Davis (1989) states that UP is the main factor that has a direct effect on UI. It also determines a large proportion of UA, and mediates the effect of FUP on UI. It also points out that the FUP influences the UP. On the other hand, the TAM establishes that AU is a function of the UP and the FUP, while the UI is linked to the UA and the UP. In this line it can be indicated that the TAM reflects the predisposition of an individual to respond favorably or unfavorably to a specific behavior.

The last two decades have provided substantial empirical support for TAM (Venkatesh & Bala, 2008). It is even considered robust, parsimonious, and influential in issues related to the adoption of Information Systems and Information Technologies (Sternad & Bobek, 2013), as well as Information and Communication Technologies (Muñoz, Climent, & Liébana, 2017), however it has its limitations. TAM provides less significant information of user opinions on adoption of specific systems, as it is limited to the constructs of UP and FUP (Awa *et al*., 2015).

Therefore, some studies have been extended to the examination of the background of the perceived variables, usefulness, and ease of use (Sternad & Bobek, 2013), that is, the two main reasons that determine acceptance according to the TAM (Sánchez, Rondán, & Villarejo, 2007), to adjust to the context of the user in order to achieve a deeper understanding of the variables that have a better predictive power.

In this line, for the purposes of the study, the integrity variable is incorporated, understood as trust in the privacy and security of the information provided in virtual social networks. This responds to the fact that these are an especially vulnerable field for the privacy of the individual (Antón, 2012; Roig, 2009), since they enable the collection of data of all kinds (Díaz, 2013).

On many occasions, virtual social networks favor the making public of data or information that traditionally had a private or reserved nature (Gandasegui, 2011; Osorio *et al*., 2016), therefore, are an especially vulnerable field for privacy (Osorio *et al*., 2016; Roig, 2009).

5. Material and methods

The research work was developed in the students of the Universidad Veracruzana of the Faculty of Accounting and Administration of the Xalapa region. The study design was non-experimental with correlational scope. This was a quantitative cross-sectional research carried out during the 2021 period.The objective of the study was to determine indices of factors that explain the use of social networks in university students, aimed at students of the 2017, 2018 and 2019 generation of the educational programs of Accounting, Administration, Administrative Computer Systems and, Management and Business Management.

Also with the aim of analyzing the state of knowledge about security vulnerabilities in social networks, a non-experimental descriptive methodological design was proposed since the study focuses on the quantitative analysis of good practices in the issue of security in the use of social networks. Subsequently, based on the results of the pilot test, the survey was validated as an instrument for collecting potential information, considering a population sample calculation. The community that makes up the faculty is 3,262 members, of which 3,024 are students (Ricárdez, 2021). Of the total number of students, only students of the 2017, 2018 and 2019 generations of the four careers offered by the faculty were considered, and from these, a finite population sample calculation was made, based on the population of enrollment registered in the period August 2020 – January 2021 (contingency adjustment September 2020 – February 2021).

ISSN-On line: 2539-1372

For this, the following formula was used:

$$n = \frac{(Z^2 * N * P * Q)}{e^2 (N-1) + z^2 * P * Q} \quad (1)$$

were:
n=Sample size searched
N=Population size
Z=Statistical parameter depending on confidence level
e=Maximum accepted estimation error
p=Probability of the event studied occurring
q=Probability that the studied event will not occur

Having the finite sample formula and the confidence level, the following calculation is made with the aforementioned data.

$$n = \frac{(Z^2 * N * P * Q)}{e^2 (N-1) + z^2 * P * Q}$$

$$n = \frac{(1.64^2 * 1982 * 0.5 * 0.5)}{e0.05^2 (1982-1) + 1.64^2 * 0.5 * 0.5}$$

$$n = \frac{1332.6968}{5.6249}$$

$$236.92 \approx 237 \pm 240$$

When obtaining the results of the formula, it can be commented that the total of respondents is 240 students of the Faculty of Accounting and Administration, of which 46 were students of the educational program of Administrative Computer Systems, 91 students of Administration, 24 students of Management and Business Management, and finally 79 students of Accounting.

In the same way in which the population sample was carried out, the pilot test was carried out, in this case, 10% of the total respondents were carried out, that is, 24 students of the Faculty of Accounting and Administration must be surveyed, of which 5 students of the educational program of Administrative Computer Systems must be, 9 students of Administration, 8 students of Accounting and finally 2 students of Management and Business Management.

Through surveys applied to students, the necessary questions were asked to analyze the knowledge about the security that users of the university community have in social networks, considering parameters such as:

a) Use of social networks. In order to determine which is the most used social network and the time spent on social networks by university students.

b) Knowledge of prevention measures. In order to know if they apply measures to improve the security of their social networks through the password they use, the knowledge they have regarding privacy policies and their application; and if they know the care protocols in case of being in a situation of risk.

c) Perception of social networks. The main idea is to know if they consider social networks safe or not.

d) Degree of personal information that the user provides on social networks. The purpose is to be able to evaluate the level of trust that the student has with the users with whom he relates, the type of content he publishes (videos, texts, photographs, among others) and the degree that the content he publishes affects third parties.

e) Vulnerabilities in social networks. With the intention of being able to establish which are the most present risk situations within social networks.

Based on the defined objective, the data of the eighteen questions with a five-point Likert scale yielded a Cronbach's alpha coefficient (α=0.9268) that exposed the existence of a direct and positive dependence between the variables perceived ease of use, perceived utility, attitude of use, intention to use social networks and integrity.On the other hand, Factor Analysis was proposed with the Principal Components method as a multivariate technique to analyze and generate factors that explain the use of social networks since it has been used to know the interdependence of variables that define the uses of social networks (Sánchez & Mestre, 2016).

6. Analysis of results

As already mentioned, the form was made to the 240 students of the Faculty of Accounting and Administration of the four educational programs, of which a greater response of the female gender was obtained with 57.9% of responses and 42.1% of the male gender.

ISSN-On line: 2539-1372

91.29% of the students indicated that they had internet at home and only 8.71% indicated that they lacked the service at home. The access points outside the home with the highest use were school (86.41%), followed by the rent plan (48.08%), public networks (27.53%) and work (20.91%).

100% of the students indicated that they were enrolled in a virtual social network. The device par excellence to access was the mobile phone (99.30%), followed by the laptop (68.64%) and, Ipad (21.60%); only 3.48% indicated that they accessed via desktop, Iwatch, PlayStation 4, Wii and Xbox.

As for the popularity of virtual social networks expressed in number of users, the data showed the following: Facebook 238, WhatsApp 237, Instagram 193, YouTube 176, Google + 145, Twitter 110, Snapchat 108, Skype 90, Pinterest 56, Line 26, Telegram 21 and LinkedIn 12. In relation to accesses per day by type of social network, the data indicated that in the category more than 12 accesses, Whatsapp (80.43%) and Facebook (53.02%) were concentrated. Meanwhile, in the category between 1 and 4 accesses were concentrated Google + (68.99%), Snapchat (57.14%), Twitter (54.37%), Skype (80.33%), Pinterest (77.19%), Line (63.16%), Telegram (77.78%) and LinkedIn (76.92%). On Instagram and YouTube, no concentration of data was found in any particular category.

In order to minimize the number of variables with high loads by one factor and thereby improve interpretation, rotation (orthogonal) was performed with the Varimax method (Kaiser, 1958; Sánchez & Mestre, 2016), the results of which are shown in Table 1.

Factor	Variance	Difference	Proportion	Accumulated
1	3.67988	0.33817	0.2044	0.2044
2	3.34172	0.12980	0.1857	0.3901
3	3.21192	0.41126	0.1784	0.5685
4	2.80066	0.00000	0.1556	0.7241

Table 1 Explained proportion of variance standardized by factor
Source: Own Elaboration

For factor reduction, factor loads were analyzed in terms of absolute values; when its value approached 1, the variable was fully explained and if it approached 0, the factors did not explain the variability (Guerrero, Hernandis, & Agudo, 2018; Rodriguez & Mora, 2001).

The data presented in Table 2 showed that the statistically significant factor loads (greater than 0.50) with positive values of Factor 1 corresponded to the variable Integrity, from Factor 2 to the variable Perceived Ease of Use, from Factor 3 to the variables Perceived Utility and Attitude of Use, while Factor 4 to the variable Intention to Use.

Variable	Factor 1	Factor 2	Factor 3	Factor 4	Exclusion
MAGP1		0.8519			0.2259
MAGP2		0.8726			0.2284
MAGP3		0.8713			0.1857
MAGP4		0.8344			0.2429
UP 1			0.6828		0.3816
UP 2			0.7106		0.4136
UP 3			0.7779		0.2787
TO 1			0.7011		0.3275
TO 2			0.5558		0.4731
TO 3			0.6872		0.2891
IT 1	0.8004				0.3213
IT 2	0.8535				0.2453
IT 3	0.8229				0.2625
IT 4	0.8366				0.2643
IT 5	0.8294				0.2784
IU 1				0.8503	0.1979
IU 2				0.8678	0.1536
IU 3				0.8162	0.1960

Table 2 Factorial loads of rotated (orthogonal) factors with the Varimax method
Source: Own Elaboration

Based on the above results, indices of the four factors were constructed as shown in Table 3. These were scaled between 0 and 100 for greater understanding of these, and were conceptualized as follows: Factor 1 "Integrity", Factor 2 "Ease of Use", Factor 4 "Attitude" and Factor 4 "Intention". The data corresponding to the indices of each of the factors were divided into quartiles for analysis purposes by means of contingency tables with row percentages.

Index	Stratum	Cuartiles (%)				Total
		1	2	3	4	
Ease of use	TO	27.13	27.91	20.16	24.80	100
	CO	26.74	17.44	24.42	31.40	100
	GD	13.33	30.00	40.00	16.67	100
	SC	23.81	28.57	30.95	16.67	100
Attitude	TO	27.91	21.71	26.36	24.02	100
	CO	22.09	27.91	26.74	23.26	100
	GD	30.00	20.00	23.33	26.67	100
	SC	19.05	33.33	19.05	28.57	100
Integrity	TO	31.78	24.03	21.71	22.48	100
	CO	12.79	30.23	31.40	25.58	100
	GD	26.67	26.67	23.33	23.33	100
	SC	28.57	16.67	23.81	30.95	100
Intention	TO	32.56	27.13	20.93	19.38	100
	CO	24.42	18.60	27.91	29.07	100
	GD	20.00	16.67	33.33	30.00	100
	SC	7.14	38.10	26.19	28.57	100

Table 3 Distribution of indices by stratum
Source: Own Elaboration

ISSN-On line: 2539-1372

With regard to the "Ease of Use" index, only the data corresponding to the students of the Accounting strata, as well as Management and Business Management were concentrated in quartiles 3 and 4.

This suggested that only in the students of these strata the use of virtual social networks was clear and understandable. In addition, only they considered that learning to use them was easy because they have the necessary skills. On the other hand, the results of the "Attitude" index showed that the highest scores of the indices of the four strata are located in quartiles 1 and 2. This suggested that in general terms most students considered the use of virtual social networks not very useful, that it did not improve their productivity and that it was not a pleasant experience and a good idea.

The results of the "Integrity" index showed that students from the strata of Administration, as well as Management and Business Management had less confidence in the information they provide to virtual social networks due to the use they can give to it, also, they do not believe in the security function they have. In general, they considered that virtual social networks are not totally reliable since the data are concentrated in quartiles 1 and 2. This contrasts with the results obtained by students from the Accounting and Administrative Computer Systems strata, since most of the data were located in quartiles 3 and 4.

The results of the "Intention" index showed that students from all strata except Administration intended to use virtual social networks in everyday activities. They also indicated that they would use and recommend them for use to the extent possible because the data were concentrated in quartiles 3 and 4.
Likewise, it was obtained that the most used social network by students is WhatsApp having a percentage of 39.6%, then 28.8% of use of Instagram, Facebook with 26.7% and finally the least used social network was Twitter with 5% (figure 1).

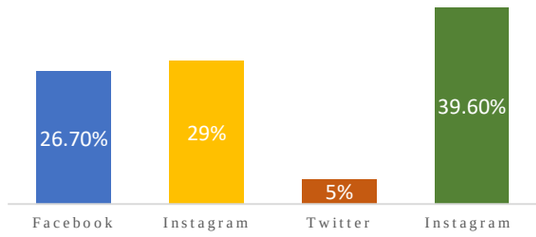

Figure 1 Percentage of social media use among university students

WhatsApp is mostly used since, with that social network, students can have greater communication in a more accessible and fast way either with their family or friends.

As a first security measure you have in social networks and email accounts, you have the access password, which is recommended to be different for each account. However, 35% of students use the same password both in their social networks and in their email accounts, so it can be a security problem, it is generally recommended to change the password for greater security at least every 2 months, we have 32% who have some similar passwords, 21% keep the passwords of all their social networks different giving this greater security to their information and thus preventing Any hack, and finally with 12% use a password for social networks and another for email in this way they feel more secure their mail and their social network (Figure 2).

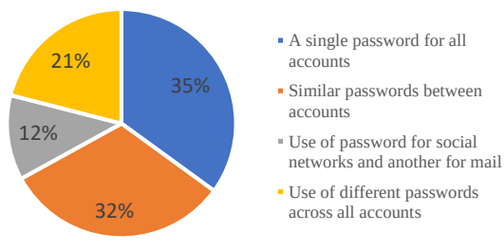

Figure 2 Using passwords in personal accounts

As noted, there is a risk factor for students, since keeping their same password for all social networks could cause their account to be hacked and their privacy may be compromised. On the other hand, each of the social networks establishes privacy rules in order to ensure that they are a safe space, where users can express themselves with confidence and there is greater control of the data by users.

ISSN-On line: 2539-1372

However, 48.3% of students have not read any privacy rules of their social networks, being an important factor, since there you can see what they do with the data and information that users publish on social networks; At the same time, 40% examine the rules of some social networks, 8.3% analyze them with the aim of making sure they can publish and 3.3% have no idea of the risk of not knowing the rules (Figure 3).

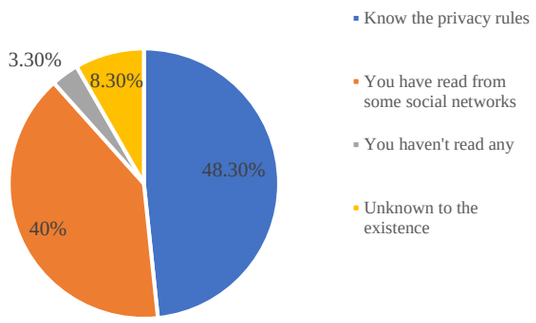

Figure 3 Knowledge of social media privacy rules

Despite the fact that, 85% of students think that social networks are not safe, it can be said that the use of them is extremely inappropriate. Although 53.8% of students have not suffered any risk situation, 46.20% have been faced with any of these situations, being mostly harassment with 44%; which is not only painful and unpleasant for the person who suffers it but also risky. At the same time, other types of situations that were identified were bullying (insults) with 28%, threats with 12% and blackmail with 16%.

Students who saw these situations before comment that they came to feel fear and even hesitated about sharing what they were experiencing at that moment with someone; resulting in great insecurity with their classmates, family and / or teachers.

Figure 4 presents an analysis of the risk situations in which students have been found, by gender. Based on the graph, it can be affirmed that 73% of risk situations occur in women, with harassment prevailing with 37%; while, in the male gender, bullying is higher, with 11.50%. And in a lower percentage in both genders is blackmail with uploading photographs, it could be considered that the latter is due to the recent Olimpia Law which, imposes penalties of up to six years for disseminating images without the consent of the person involved.

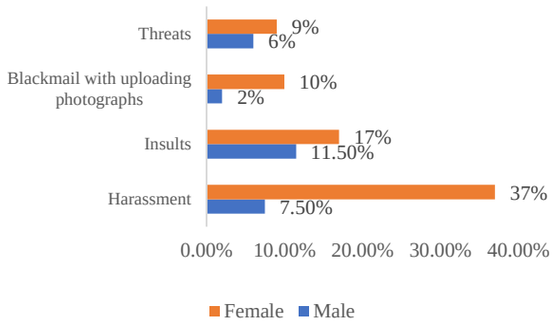

Figure 4 Threat analysis by gender

7. Conclusion

Social networks have transformed the way people communicate, being tools that facilitate the exchange of information among their users through publications and text messages, videos, images, among others. However, the large amount of data that is exposed in them, makes them so vulnerable, to the extent that it is not possible to guarantee total security for the user. The findings showed that the use of virtual social networks has a multidimensional behavior composed of the factors called: Integrity, Ease of Use, Attitude and Intention. When scanned and analyzed by quartiles, the four factors showed different behavior in the different strata.

Although the results showed that the highest scores of the Attitude indices of the four strata were located in quartiles 1 and 2, there is a wide use of virtual social networks, especially Facebook and WhatsApp, using the mobile phone as the means of connection par excellence.

The above could indicate that even when each generation uses certain social networks and makes different use of them, according to their interests and tastes; From various angles, its use in the 4 strata could be related to satisfying other needs such as social inclusion, belonging, curiosity or social recognition.

Likewise, the results showed that the strata of Accounting, Management and Business Management, as well as Administrative Computer Systems had high rates of Intention, which is consistent if the age ranges in which they are located are analyzed; These are individuals who can be considered as digital natives.

ISSN-On line: 2539-1372

In contrast, in the Administration program, the low Intention index is not explained by age ranges, that is, they are not digital immigrants, but rather because they have a lower Integrity index, that is, low level of confidence in the information they provide to social networks, due to the use they can give to it and the security function they possess.

Although students from the four strata can be considered as digital natives, the data show that they may require better training in terms of digital literacy regarding the use of social networks, especially those who belong to the layers of Administration and Administrative Computer Systems.

On the other hand, security has become a fundamental issue since, people can not move away from sharing a photo, video or publication on their social networks. While it is true that social networks maintain certain privacy notices, to give some security and confidence to users, this does not entirely guarantee user protection; Because the location, interests and photographs that are shared in them, are analyzed by the same application to show certain advertising of interest to it.

As the main reason why users do not protect their privacy, is because they are not sufficiently aware and responsible of the value of their information. Large companies like Facebook and Instagram are millionaires thanks to the data they know, for example; What you do, you like, who are our friends and our family, where you go on vacation, where you study or work. They may analyze this information so that they can display corresponding advertising for products or services that are of interest, as well as offer notes and other information articles that they know are more interesting. (Pastorino, 2018)

That is why what is published on social networks must be better protected, because, just as it can be something positive, it can attract serious problems with personal and family safety; Being exposed through the information published to different attacks and vulnerabilities such as: blackmail, harassment, impersonations, threats, among others.

In the understanding that, 48.3% of students do not know how to proceed in cases of insecurity in their social networks and 74.2% do not even know who they can go to in case of being in a situation of risk, to grant informative talks about the rules of security and privacy of social networks, It will reduce risks and provide faster care.

Based on surveys, one of the main topics to be discussed with college students should be the handling of data confidentiality, because a high percentage have little knowledge about how to provide greater protection against theft of data found on their networks; The clearest example of this is the fact that they mostly maintain the same password for all their accounts with a basic security level, when on the contrary, it is advisable to change monthly or annually the password that includes letters, numbers, and some allowed symbol.

Although, social networks follow a basic security protocol to prevent people outside the account from entering them; the amount of personal information they allow to enter, makes them vulnerable and less secure; since, if the account is compromised or the information is not properly privatized, the user is exposed and vulnerable before cybercriminals (Cragno, *et al*., 2018).

Finally, the findings of the study could have implications in various aspects in the field of Social Sciences, especially in the delineation of a profile of Internet users who are digital natives training in business issues in a framework where the evolution of virtual social networks prints an enormous dynamism and whose limits are difficult to estimate.

In this sense, it is also necessary to instruct students on the various measures that exist to prevent social engineering attacks, such as those mentioned by INCIBE (2016) of: not opening emails with unknown users, not answering any suspicious email where they ask for any personal information, not opening links that send to personal email, WhatsApp or social network, have an antivirus and do not connect to open WIFI networks. As well as these measures there are more, which allow to protect against social engineering and thus prevent cybercriminals from stealing confidential data.

ISSN-On line: 2539-1372

8. References

Aced, C. (2010). Social networks in a week. Grupo Planeta (GBS).

Antón, A. (2012). The phenomenon of social networks and changes in the validity of Fundamental Rights. Revista de Derecho de la UNED (RDUNED), (10), 209–255. http://e-spacio.uned.es/fez/view/bibliuned:RDUNED-2012-10-5090

Arab, E.; Díaz, A. (2015). Impact of social networks and the internet on adolescence: positive and negative aspects. Revista Médica Clínica Las Condes, 26(1), 7–13. https://doi.org/https://doi.org/10.1016/j.rmclc.2014.12.001

Awa, H.; Ojiabo, O.; Emecheta, B. (2015). Integrating TAM, TPB and TOE frameworks and expanding their characteristic constructs for e-commerce adoption by SMEs. Journal of Science and Technology Policy Management, 6(1), 76–94. https://doi.org/10.1108/JSTPM-04-2014-0012

Ben, K. (2016). An analysis of business' acceptance of internet banking: an integration of e-trust to the TAM. Journal of Business & Industrial Marketing, 31(8), 982–994. https://doi.org/10.1108/JBIM-10-2016-271

Blas, S.; Mafé, C.; Manzano, J. (2008). The influence of the dependence of the medium on B2C e-commerce. Proposal of an integrative model applied to the intention of future purchase on the Internet. Cuadernos de Economía y Dirección de la Empresa, 11(36), 45–75. https://www.sciencedirect.com/science/article/pii/S113857580870063X

Buxarrais, M. (2016). Redes sociales y educación. Education in the Knowledge Society, 17(2), 15–20. https://doi.org/10.14201/eks20161721520

Caldevilla, D. (2010). Social networks. Typology, use and consumption of 2.0 networks in today's digital society. Documentation of Information Sciences, 33, 45-68. http://agora.edu.es/servlet/articulo?codigo=3250105

Casaló, L.; Flavian, C.; Guinalíu, M. (2012). Virtual social networks developed by business organizations: background of consumer engagement intent. Cuadernos de Economía y Dirección de la Empresa, 15(1), 42–51. https://doi.org/10.1016/j.cede.2011.06.003

Castro, To.; Moral, M. de la V. (2017). Problematic use of social networks 2.0 in digital natives: bibliographic analysis. Health and Drugs, 17(1), 73–85. https://www.redalyc.org/pdf/839/83949782008.pdf

Celaya, J. (2000). The company in Web 2.0. Ediciones Gestión 2000.

Cronbach, L. (1951). Coefficient alpha and the internal structure of tests. Psychometrika, 16(3), 297–334. https://link.springer.com/article/10.1007/bf02310555

Cragno, A., Duarte Tau, N., Mamani, K., & Papa, J. (2018) Computer Security in Social Networks. In National Congress of Computer Engineering / Information Systems CoNaIISI. National Technological University. https://grupogemis.com.ar/wp-content/uploads/2018/11/SyO_M_SegInfRedesSociales.pdf

Cruz, A. (November 5, 2020). So you can turn on temporary messages on WhatsApp. El Universal. https://www.eluniversal.com.mx/techbit/whatsapp-ya-habilito-los-mensajes-temporales-asi-funcionan

Davis, F. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS quarterly,13 (3), 319–340. https://doi.org/10.2307/249008

Davis, F.; Bagozzi, R.; Warshaw, P. (1989). User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. Management Science, 35(8), 982–1003. https://doi.org/10.1287/mnsc.35.8.982

Del Barrio, Á.; Ruíz, I. (2016). Teenagers and the use of social networks. International Journal of Developmental and Educational Psychology. INFAD Journal of Psychology., 3(1), 571–576. https://doi.org/10.17060/ijodaep.2014.n1.v3.537

ISSN-On line: 2539-1372

Díaz, A. (2013). Self-regulation in social networks as a way to guarantee the rights of intimacy, privacy and protection of personal data. Derecom, (13), 125–143. https://dialnet.unirioja.es/servlet/articulo?codigo=4330473

Dominguez, F.; López, R. (2015). Use of digital social networks among young university students in Mexico. Towards the construction of a state of knowledge (2004-2014). Journal of Communication, (14), 48–69. https://dialnet.unirioja.es/servlet/articulo?codigo=5223798

Fishbein, M.; Ajzen, I. (1975). Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research. Addison-Wesley Publishing Company

Forbes. (January 28, 2014). Risk and vulnerability in social networks. Forbes Mexico. https://www.forbes.com.mx/riesgo-y-vulnerabilidad-en-las-redes-sociales/

Gandasegui, V. (2011). Myths and realities of social networks. Social Prism: Journal of Social Research, (6), 340–366. https://www.redalyc.org/pdf/3537/353744578007.pdf

Gangwar, H.; Date, H.; Ramaswamy, R. (2015). Understanding determinants of cloud computing adoption using an integrated TAM-TOE model. Journal of Enterprise Information Management, 28(1), 107–130. https://doi.org/10.1108/JEIM-08-2013-0065

Garcia, And.; Nazareth, H. (2017). Emotions and social networks in adolescents. Journal of Studies and Research in Psychology and Education, (13), 11–15. https://doi.org/https://doi.org/10.17979/reipe.2017.0.13.2131

Garcia, M.; Dry, J.; Del Hoyo, M. (2013). The participation of young people in social networks: purpose, opportunities and rewards. Anàlisi Monogràfic, (48), 95–110. https://doi.org/10.7238/a.v0iM.1968

Gomez, M.; Roses, S.; Farias, P. (2012). The academic use of social networks in university students. Comunicar, 19(38), 131–138. https://doi.org/10.3916/C38-2012-03-04

Guerrero, M.; Hernandis, B.; Acute, B. (2018). Approach to the representation of the shape and appearance of the product: study on the design attributes. Innovate, 28(67), 25–39. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0121-50512018000100025

INTECO-AEPD. (2009). Study on personal data privacy and information security in online social networks. (February 2009 Report). https://www.uv.es/limprot/boletin9/inteco.pdf

INCIBE. (August 8, 2016). How to combat social engineering? National Institute of Cybersecurity INCIBE. https://www.incibe.es/protege-tu-empresa/blog/combatir-ingenieria-social-este-empresario-nos-cuenta

INCIBE. (March 20, 2017). Threat vs Vulnerability, do you know how they differ? National Institute of Cybersecurity INCIBE. https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian#:~:text=Una vulnerability

Jasso, J. L.; Lopez, F.; Díaz, R. (2017). Addictive behavior to social networks and its relationship with problematic mobile use. Psychological Research Act, 7(3), 2832–2838. https://doi.org/10.1016/j.aipprr.2017.11.001

Jones, C.; Motta, J.; Alderete, M. (2016). Strategic management of information and communication technologies and adoption of electronic commerce in MSMEs in Córdoba, Argentina. Management Studies, 32(138), 4–13. https://doi.org/10.1016/j.estger.2015.12.003

Jordan, V.; Galperin, H.; Peres, W. (2010). Accelerating the digital revolution: broadband for Latin America and the Caribbean. ECLAC. http://hdl.handle.net/11362/2972

Kaiser, H. (1958). The varimax criterion for analytic rotation in factor analysis. Psychometrika, 23(3), 187–200. https://link.springer.com/article/10.1007/BF02289233

Kaiser, H. (1960). The application of electronic computers to factor analysis. Educational and psychological measurement, 20(1), 141–151. https://doi.org/10.1177/001316446002000116

ISSN-On line: 2539-1372

López, P. (2004). Sample population and sampling. Point zero, 9(08), 69–74. http://www.scielo.org.bo/pdf/rpc/v09n08/v09n08a12.pdf

Lorenzo, C.; Gomez, M.; Alarcón, M. (2011). Virtual social networks, what does their use depend on in Spain? INNOVATE. 21(41), 145-157. https://revistas.unal.edu.co/index.php/innovar/article/view/35398/35766

Martinez, C. (2018). Use of social networks in the scientific journals of the University of Los Andes, Venezuela. Information Sciences, 8(1), 32–52. http://dx.doi.org/10.15517/eci.v8i1.28104

Muñoz, F.; Climent, S.; Liébana, F. (2017). Determinants of intention to use the mobile banking apps: An extension of the classic TAM model. Spanish Journal of Marketing - ESIC, 21(1), 25–38. https://doi.org/https://doi.org/10.1016/j.sjme.2016.12.001

Olmo, L. (31 May 2017). Phishing attacks are no longer executed by email but on social networks. Noti_infosegura: Social media, the most effective means for phishing attacks. https://www.uv.mx/infosegura/general/noti_phishing-21/

Osorio, M. J.; Molero, M. del M.; Pérez, M. del C.; Mercader, I. (2016). Social networks on the internet and consequences of their use in university students. International Journal of Developmental and Educational Psychology. INFAD Journal of Psychology., 3(1), 585–592. https://dehesa.unex.es/handle/10662/1901

Ponce, I. (2012, April). Social networks - classification of social networks. http://recursostic.educacion.es/observatorio/web/en/internet/web-20/1043-redes-sociales?start=3

Pastorino, C. (21 March 2018). Social networks: the value of personal information and the responsibility of users. Welivesecurity. https://www.welivesecurity.com/la-es/2018/03/21/redes-sociales-valor-informacion-responsabilidad-usuarios/

Ricárdez, J. (2021). PLADEA 2017-2021. Universidad Veracruzana. https://www.uv.mx/fca/files/2018/09/PLADEA_2017-2021.pdf

Prensky, M. (2001). Digital Natives, Digital Immigrants Part 1. On the Horizon, 9 (5), 1-6. https://doi.org/10.1108/10748120110424816

Rodriguez, I.; Herrero, Á. (2008). Background of the perceived usefulness in the adoption of electronic commerce among individuals and companies. Cuadernos de Economía y Dirección de la Empresa, 11(34), 107–134. https://doi.org/https://doi.org/10.1016/S1138-5758(08)70055-0

Rodriguez, M.; Mora, R. (2001). Computer statistics: cases and examples with the SPSS. University of Alicante.

Roig, A. (2009). E-privacy and social networks. Journal of Law and Political Science Studies of the UOC, (9), 42–52. https://dialnet.unirioja.es/servlet/articulo?codigo=3101802

Romero, C.; De Amo, M.; Borja, M. (2011). Adoption of virtual social networks: expansion of the technological acceptance model integrating trust and perceived risk. Cuadernos de Economía y Dirección de la Empresa, 14(3), 194–205. https://doi.org/10.1016/j.cede.2010.12.003

Sanchez, M.; Rondán, F.; Villarejo, Á. (2007). An empirical model of adaptation and use of the Web. Perceived utility, ease of use and flow. Cuadernos de Economía y Dirección de la Empresa, 10(30), 153–179. https://doi.org/https://doi.org/10.1016/S1138-5758(07)70077-4

Sanchez, S.; Mestre, R. (2016). Social networks and university students: uses and personal identity. Journal of Human and Social Sciences, (10), 696–714. https://dialnet.unirioja.es/servlet/articulo?codigo=5875192

Sandoval, R.; Romero, To.; Heredia, E. (2013). Communication and exchange with social networks in university education: case students of Administration and Computer Science. Electronic Journal Apertura, 5(2), 1–30. https://www.redalyc.org/pdf/688/68830444008.pdf

Santos, F. R. (1989). The concept of social network. Reis, 48 137-152. https://doi.org/10.2307/40183465

Santos, M. (2010). Social network analysis and academic performance: lessons from the case of the United States. Debates in Sociology, (35), 7–44. https://revistas.pucp.edu.pe/index.php/debatesensociologia/article/view/2125

Shin, D. (2008). Understanding purchasing behaviors in a virtual economy: Consumer behavior involving virtual currency in Web 2.0 communities. Interacting with computers, 20(4–5), 433–446. https://doi.org/10.1016/S0953-5438(08)00025-8

Sternad, S.; Bobek, S. (2013). Impacts of TAM-based external factors on ERP acceptance. Procedia Technology, 9, 33–42.

Torres Clara ravine. (2014). Cyberbullying: concept and educational aspects [Final Degree Project in Pedagogy, University of Granada]. http://digibug.ugr.es/bitstream/handle/10481/36357/BarrancoTorres_TFG.pdf?sequence=1&isAllowed=y

UNAM. (2009). Security on social networking sites. Security Magazine (0). https://revista.seguridad.unam.mx/numero-0/seguridad-en-los-sitios-de-redes-sociales

Usla, H. (May 7, 2020). COVID-19 gives a 42% "high" to social media use: Nielsen IBOPE. The Financier. https://www.elfinanciero.com.mx/economia/covid-19-le-da-un-subidon-de-42-al-uso-de-las-redes-sociales-nielsen-ibope

Venkatesh, V.; Bala, H. (2008). Technology Acceptance Model 3 and a Research Agenda on Interventions. Decision Sciences, 39(2), 273–315. https://doi.org/10.1111/j.1540-5915.2008.00192.x

Willis, T. (2008). An evaluation of the technology acceptance model as a means of understanding online social networking behavior. University of South Florida.

ISSN-On line: 2539-1372