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

https://doi.org/10.23913/ride.v12i23.980

Artículos científicos

Aplicaciones educativas digitales y la falta de seguridad de los datos personales de sus usuarios

Lack of Security of the Personal Information in Educational Digital Applications

Aplicações educacionais digitais e a falta de segurança dos dados pessoais de seus usuários

Paola Iliana de la Rosa Rodríguez
Universidad Autónoma de San Luis Potosí, México
paola.delarosa@uaslp.mx
https://orcid.org/0000-0001-6620-3589

Resumen

Este artículo analiza el uso de plataformas digitales en jóvenes universitarios y su conocimiento sobre los riesgos de exponer su información en estos espacios. Además, estudia el tratamiento de la información por diversas aplicaciones de uso didáctico. Para lograr lo anterior, se realizó un estudio exploratorio e inferencial y se aplicó una encuesta semiestructurada a alumnos de Criminología de la Universidad Autónoma de San Luis Potosí (UASLP). Asimismo, se eligieron 29 plataformas educativas y se analizó si protegen los datos de los usuarios, al igual que, en caso de hacerlo, el alcance de dicha protección. Los resultados evidenciaron que no existen mecanismos que protejan la privacidad y seguridad de la información que manejan las aplicaciones y que la responsabilidad por el mal uso de la información reside en los usuarios. También se encontró que el conocimiento y práctica de métodos para preservar la seguridad cibernética por parte de los internautas de las plataformas educativas tiene relación directa con dicha seguridad, por lo que hace falta un mayor conocimiento de herramientas para proteger los datos personales en el ciberespacio.

Palabras clave: ambientes educacionales, cibercrimen, plataformas virtuales, protección de datos, tecnología educativa.

Abstract

This article analyzes the use of digital platforms in young university students and their knowledge about the risks of exposing their information in these spaces. In addition, it studies the treatment of information by various applications for didactic use. To achieve this, an exploratory and inferential study was carried out and a semi-structured survey was applied to Criminology students from the Universidad Autónoma de San Luis Potosí (UASLP). Likewise, 29 educational platforms were chosen, and it was analyzed whether they protect user data, as well as, if they do, the scope of said protection. The results showed that there are no mechanisms to protect the privacy and security of the information handled by the applications and that the responsibility for the misuse of the information resides with the users. It was also found that the knowledge and practice of methods to preserve cyber security by Internet users of educational platforms is directly related to said security, which is why a greater knowledge of tools is needed to protect personal data in cyberspace.

Keywords: educational environment, cybercrime, virtual platforms, personal information protection, educational technology.

Resumo

Este artigo analisa o uso de plataformas digitais por jovens universitários e seus conhecimentos sobre os riscos de expor suas informações nesses espaços. Além disso, estuda o tratamento da informação por diversos aplicativos de uso didático. Para tanto, foi realizado um estudo exploratório e inferencial e aplicado um questionário semiestruturado a alunos de Criminologia da Universidade Autônoma de San Luis Potosí (UASLP). Da mesma forma, foram escolhidas 29 plataformas educacionais e foi analisado se protegem os dados dos usuários, bem como, caso o façam, o alcance dessa proteção. Os resultados mostraram que não existem mecanismos de proteção à privacidade e segurança das informações tratadas pelos aplicativos e que a responsabilidade pelo uso indevido das informações é dos usuários. Constatou-se também que o conhecimento e a prática de métodos de preservação da segurança cibernética pelos internautas de plataformas educacionais está diretamente relacionado a essa segurança, razão pela qual é necessário um maior conhecimento das ferramentas de proteção de dados pessoais no ciberespaço.

Palavras-chave: ambientes educacionais, crimes cibernéticos, plataformas virtuais, proteção de dados, tecnologia educacional.

Fecha Recepción: Enero 2021 **Fecha Aceptación:** Julio 2021

Introduction

The pedagogy taught through printed documents and the blackboard is nowadays being replaced by virtual environments that adapt to the teaching-learning styles of teachers and students and that favor collaborative learning, interactivity and interdisciplinarity (Quintero, Munévar and Álvarez, 2009). Following Gallado, Marqués and Bullen (2014), it is unavoidable to transmute classrooms into more attractive, participatory and productive learning spaces.

In the educational context, digital environments are seen as mass media capable of sharing a message almost immediately and with a wide capacity to store data. Through them distances are shortened and information is available at any time, as long as you have access to an electronic device connected to the Internet. According to López (2007), it was from the 80's when In the university environment, information and communication technologies (ICT) began to be used to a greater extent, which has led to the integration of the various tools by teachers and students in the teaching-learning processes.

Since then, technologies have caused new generations of students to acquire knowledge in a different way, since their familiarity with the digital world demands new teaching methods. In the first decade of the 21st century, as mentioned by Conde and Boza (2019), groups of students began to form with more constructive roles, prone to perform more in virtual mode than in person. They were students belonging to the so-called network generation, who were characterized by showing a close relationship with digital technologies and educational innovations. The term network generation is due to Don Tapscott (1998). In his studies on the computer revolution published in 1998, this author refers that the children of this generation have been educated in the digital society and that now, a large part of them, already of legal age, are completely immersed in the digital age.

"Youth is thus perceived as a social group closely linked to digitization and networks" (Crovi, 2010, p. 122). A generation characterized by using portable computers with an internet connection that learn through virtual communities.

For Cataldi and Dominighini (2015), people born between 1980 and 2000 developed in social contexts with technological means and now use ICTs productively. They are familiar with the use of emails, video games, social networks, digital cameras, internet search engines, video chats, geolocators and wireless systems. Electronic devices are an extension of them and even have greater technological capabilities than their masters. Negroponte (1995) specifies that each generation has been more digital than the previous one.

However, the increasing incorporation of electronic spaces in the pedagogical area, on the one hand, and the use of cyberspace by criminals, on the other, represent new challenges for current generations of students. Today, cybersecurity is an issue that reaches not only those who use the Internet for commercial purposes, but also those who open accounts on virtual platforms and use educational programs in these spaces.

Taking as a premise the risks derived from the exposure of personal data in the teaching of courses with virtual modalities, this article examines whether there is information security in educational digital environments. To find out if users are aware of the risks in cyberspace and if they adopt security mechanisms in the accounts they open for educational purposes, platforms are analyzed and an exploratory study is conducted.

The hypothesis raised by this work is that these educational tools do not offer sufficient security mechanisms, thus endangering the identity and privacy of personal information and violating the protection of personal data of students who operate in virtual communities of learning. There is no doubt that the ignorance of the security mechanisms exposes the information of the netizens in a risky way.

Materials and methods

In order to verify or discard the hypothesis, a descriptive-explanatory study was carried out first. Consequently, the information obtained from the digital tools shown in Table 1 was collected and analyzed.

Tabla 1. Relación de plataformas objeto de estudio

Blogger	Kahoot	Tes
Calendario Google	Microsoft 365	Trello
Celebrity	Mindmeister	Tumblr
DidacTIC	OneDrive (Microsoft)	Tzaloa (Moodle)
Dropbox	Padlet	WeTransfer
Easybib	Quizizz	Wikia
Edmodo	Remind	WorkFlowy
Evernote	Schoology	Wordpress
Hangouts	Stormboard	Zoho
Jumpshare	Symbaloo	

Fuente: Elaboración propia

These 29 educational platforms were selected for being the ones most frequently used by undergraduate students, according to a survey, and with the intention of identifying the processing of personal data of users of said digital environments. Thus, the particularities of these virtual spaces were analyzed with regard to the protection of the data provided by users and with respect to whether they share said information with third parties. Likewise, it was investigated who is responsible if there is a misuse of this personal data.

Subsequently, in April and May 2020, an exploratory and inferential study was carried out. As part of this phase, the survey included in figure 7 was applied to 155 students of the degree in Criminology at the Autonomous University of San Luis Potosí (UASLP). The sample included second, fourth, sixth and eighth semester students. Initially, the total number of students was 271; of them, 205 were women and 66 men, and they were between the ages of 18 and 25. Of this population, 155 answered the survey, which yielded a confidence level of 95% and a margin of error of 5%. The standard deviation with respect to the mean is 2.7.

The research instrument was a semi-structured survey (see annex) made up of 14 questions: six open questions and eight items with a Likert-type scale, that is, questions with a range of response options for the respondents to choose from. Thanks to these items, information was obtained on the frequency of handling of digital platforms, the purposes of the use of programs or virtual classrooms within the course, the security devices they use, their knowledge about the treatment that the platforms do on the data personal information and their knowledge of the privacy policies of said applications, among other aspects.

However, regarding the unobservable variable to be measured, which in this case is the security of personal data uploaded to the platforms, the following independent variables were specifically included and measured: a) the frequency with which they use devices cybersecurity, b) their knowledge about the notices and privacy policies of the platforms, c) their knowledge about the processing of personal data of the platforms and d) the semester that the student is studying. These items were chosen because they are the ones that are positively related to cybersecurity.

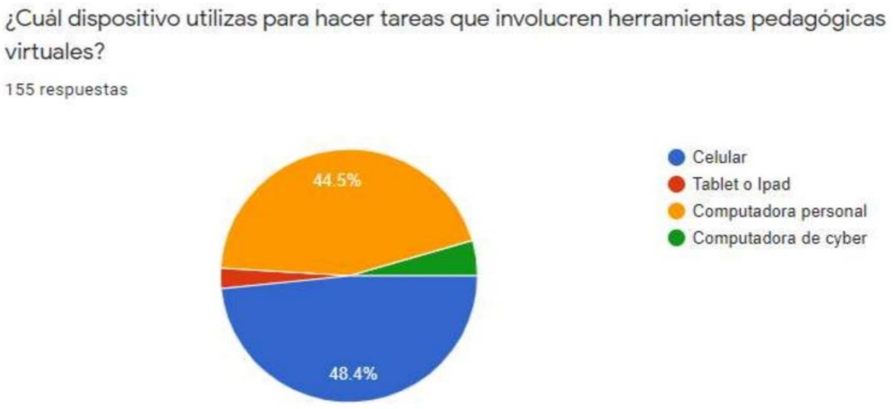
To determine the validity of the study carried out, Cronbach's alpha coefficient was used, which serves to measure the reliability of a measurement scale (Campo, 2006). It was calculated by the correlation matrix using Excel. For this, the answers to the dichotomous questions about the knowledge of notices and policies, as well as the processing of their data on platforms, were assigned the value of one if they were negative and two if they were affirmative. To assess the frequency of safety devices, the following values were assigned: 1 = Never, 2 = Very rarely, and 3 = Almost always. All values were ordered from lowest to highest. The semester of the student surveyed was also included, in order to determine if a lower semester represents less knowledge about cybersecurity.

Results

Use of platforms and cybersecurity of university students

Regarding the device that students use to do tasks that involve virtual technological tools, it was found that 48.4% of the surveyed population uses cell phones, 44.5% use personal computers, 4% rent computers and 3% own tablets or iPad, such as can be seen in figure 1.

Figura 1. Uso de dispositivos para realizar tareas



Fuente: Elaboración propia

The information obtained on the applications used by teachers is indicated in Table 2.

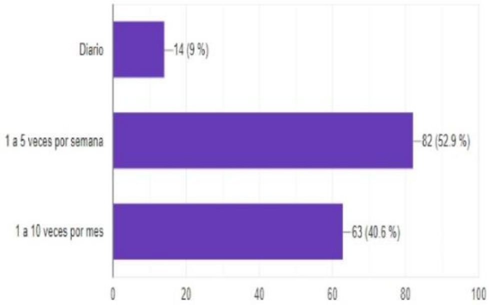
Tabla 2. Plataformas y aplicaciones que más utilizan sus profesores

Schoology	22.6 %
Tzaloa	18.7 %
DidacTIC	14.8 %
OneDrive	14.2 %
Kahoot!	11.6 %
Otras	18.1 %

Fuente: Elaboración propia

In addition, 80% of the surveyed population responded that they integrate the platforms to carry out tasks and 20% answered that they use them to prepare projects. Figure 2 shows the frequency of use of these applications by the surveyed population.

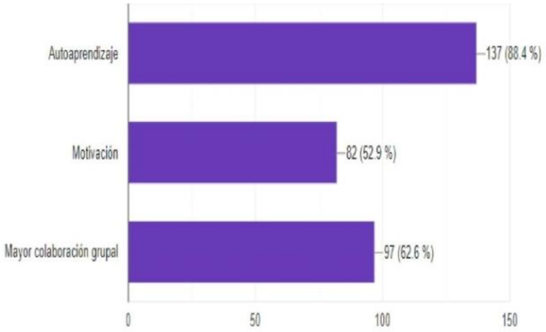
Figura 2. Frecuencia de uso de aplicaciones electrónicas



Fuente: Elaboración propia

For its part, Figure 3 shows what students are looking for when using a digital tool.

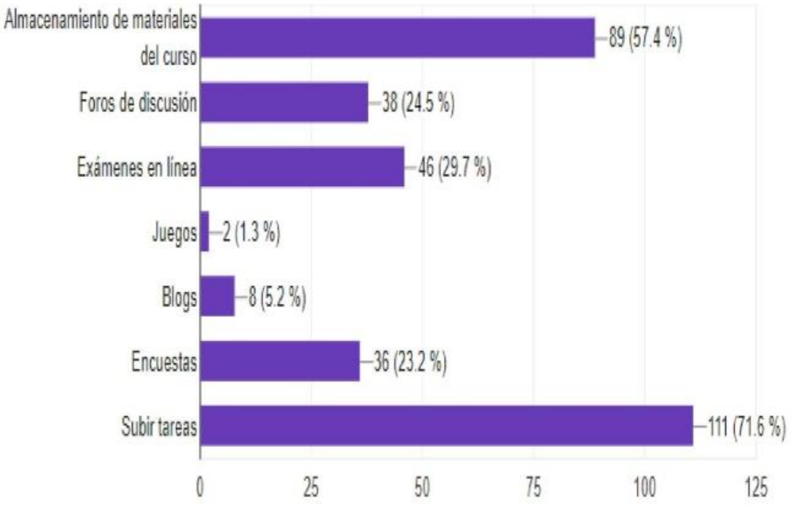
Figura 3. ¿Qué buscan obtener los alumnos al usar una herramienta digital?



Fuente: Elaboración propia

The purposes for which teachers use the platforms are listed in Figure 4.

Figura 4. Uso de las plataformas durante los cursos



Fuente: Elaboración propia

In terms of cybersecurity, 58.1% of the surveyed population says they know what it is about, while 41.9% do not know what it refers to.

The security methods known to the surveyed population are shown in Table 3.

Tabla 3. Métodos de seguridad utilizados por los estudiantes

Antivirus	36.8 %
Contraseñas	20 %
Otras	20.6 %
No las conoce	22.6 %

Fuente: Elaboración propia

The situations that put at risk or compromise the security of student data are listed in Table 4.

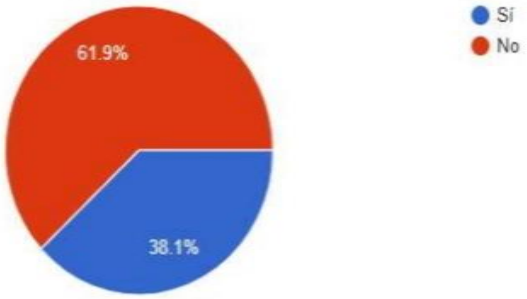
Tabla 4. Condiciones que arriesgan la seguridad de los datos personales

No cerrar apropiadamente su sesión	40.6%
Aceptar el uso de cookies	27.7%
Utilizar computadoras públicas	21.3%
Crear una cuenta	10.3%

Fuente: Elaboración propia

Most of the students state that they are aware of the processing of their personal data on the educational platforms they use (61.9%) (see figure 5).

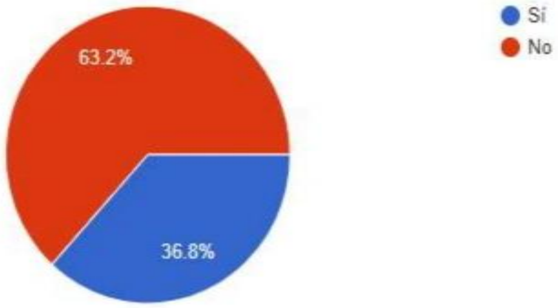
Figura 5. Estudiantes que conocen el tratamiento de las plataformas educativas hacia sus datos personales



Fuente: Elaboración propia

Regarding the notices and privacy policies of educational platforms, what was stated in figure 6 was obtained.

Figura 6. Estudiantes que conocen los avisos y políticas de privacidad de las plataformas educativas



Fuente: Elaboración propia

More than half of the students surveyed do not read the notices and privacy policies of the programs and applications and are unaware of the handling of personal information that they enter on the platforms. Likewise, 40% of the students surveyed did not refer to the security methods used, since close to this same percentage are unaware of the issue of cybersecurity. Therefore, the persistent behavioral pattern in students is that they are not informed about the destination of the personal data that enter the Internet and there is no concern of these to know and apply security mechanisms.

Regarding the unobservable variable, namely cyber security, Cronbach's alpha was used for the four items that were considered in the survey: from a sample of 155 subjects it was 0.77. This is a high grade value, so the data collection instrument that was constructed presents high reliability (Celina and Campo, 2005). The following formula was used:

$$\alpha = \frac{k}{k-1}\left[1 - \frac{\sum V_i}{V_t}\right]$$

Where the variables represent the following:

α: Cronbach's alpha.

k: Number of items.

V_i: Variance of each item.

V_t: Total variance.

Tabla 5. Estadísticos de la escala

K	Vi	Vt	α
4	6.660	15.876	0.773966601

Fuente: Elaboración propia

Table 5 shows the values of the variables in this study. The results show that there is a correlation between the cyber security of the surveyed students, which depends both on the number of semesters they have taken and the frequency of use of their devices, on the verification they make of the notices and privacy policies and knowledge of the handling of personal data by electronic platforms. The latter constitute patterns of behavior that influence the safety of users, as they are related to the risky exposure of their information through the platforms.

It is worth mentioning that the UASLP have been enabling social networks as a means of information and communication for their educational programs. As an example, in 2016 the registered courses that use the Tzaloa (Moodle) and DidacTIC platforms increased, which may have an impact on more student data being exposed to the insecurity of cyberspace. Even more, since the pandemic, Microsoft Teams is being used, as well as other applications that teachers choose.

Now, concatenating these results and because UASLP teachers rely on other electronic tools to teach their courses, this study aims to know the security mechanisms and the treatment that educational platforms have for their users.

For this study, the educational applications studied were classified as follows:

- eight tools that constitute work platforms,
- three tools to store data,
- ten tools to discuss and collaborate,
- five tools to organize work and
- three games.

Once the information from each of the 29 applications or programs was collected, we proceeded to study, quantify and analyze whether these pages offer security mechanisms. After examining the privacy policies of each company and other aspects sought in this research, the following results were obtained (see table 6).

Tabla 6. Concentrado sobre el tratamiento de datos personales en plataformas con fines educativos

	Plataformas de trabajo	Almacenamiento	Debate y colaboración	Organizadores de trabajo	Juegos	Total de plataformas
¿Comparte información de usuarios con terceros?	7	3	8	5	2	25
Requiere el consentimiento del usuario para permitir que terceras partes usen el contenido de sus datos pero lo hace a través del aviso privacidad (que pocas veces se lee).	8	2	6	4	0	20
La responsabilidad por el uso de los datos recae en el usuario o menciona que no se hace responsable	8	3	10	5	3	29
¿Regula la protección de los datos de menores de edad?	5	0	5	1	1	12

Fuente: Elaboración propia

It is noteworthy that 25 of the analyzed sites expressly state that they do share user information with third parties, even stating that they do not control or respond to how third parties can have access to their users' information. Notwithstanding the foregoing, the sites use their own cookies and accept cookies from third parties such as suppliers, marketing companies, among others, which obtain and analyze user data to adapt content, improve services and show them advertising related to their preferences through the analysis of browsing data, but with whom the user of the educational platforms did not open a personal account and of whom they do not know the destination and use that they may exercise on their data. Another important aspect is the companies that administer various services on the Internet; companies managed by Google, for example, point out that services and applications that run on a device communicate with other servers offered by the company and clarify that they can share user information with each other. In addition, the applications receive countless unknown visitors who can break these security controls.

Only 68% of the pages analyzed require consent to allow third parties to use the content of the data and, as analyzed, they do so through the acceptance of the privacy notice, a mandatory step to generate the electronic account that gives access to the site. . It is a generality that the companies that administer the platform share the data or allow servers to have access to them; What the companies point out is that, in any case, if the user wishes to deny the sharing of their personal data, the account will have to be configured for this purpose, a situation that is only possible when the page has this option.

All the analyzed pages disclaim responsibility for the misuse of the data that users enter. Specifically, 20 transfer responsibility for the misuse of the data that users enter to the user, 10 applications do not indicate who is responsible and deviate from it. It was found that certain companies transfer said responsibility to the controller, which is "the natural or legal person, public authority, agency or other body that alone, or in conjunction with others, determines the purpose and means to process personal data."

As can be seen, the general pattern of the companies that manage the platforms is to allow user data to be shared and not be responsible for the data that users enter. In addition, it is noted that each country has its policies on privacy, data transfer and applications have different rights for American, European and Latin American users, which can create confusion in this regard.

Another important fact is that younger generations are more likely than adult generations to provide personal information without major controls (Norton, 2018).

Regarding the platforms used by the surveyed population, the results were recorded in Table 7.

Tabla 7. Tratamiento de datos en las plataformas usadas por alumnos de Criminología de la UASLP

	Tzaloa	DidacTIC	Schoology	OneDrive
¿Comparte información de usuarios con terceros?	Sí	Sí	Sí	Sí
Requiere el consentimiento del usuario para permitir que terceras partes usen el contenido de sus datos pero lo hace a través del aviso de privacidad.	Sí	Sí	Sí	Sí
La responsabilidad por el uso de los datos recae en el usuario o menciona que no se hace responsable.	Sí	Sí	Sí	Sí

Fuente: Elaboración propia

The number of users of technological devices and the Internet is increasing. And as detected here, personal data insecurity rates can grow as the number of Internet users grows. The National Survey on the Availability and Use of Information Technologies in Mexican Homes (Endutih) (National Institute of Statistics and Geography [Inegi], 2018) documented that in 2018 there were 50 845 170 computer users, 74 325 379 computer users. Internet and 83 079 732 mobile phone users. According to age groups, 9,226,846, that is, 18.1% of the total netizens in the country, were users between 18 and 24 years old. In addition to this, it documented that 23,757,297 people were computer users for school work. The computer was used that year by 18,620,599 undergraduate students. Finally, 13 201590 of the cell phone users were between 18 and 24 years old.

With the above information it can be inferred that we live in a digital world where collecting and storing personal data is more the norm than the exception. While it is a given that companies collect personal information for analytics, research, advertising or marketing purposes, many times we do not know where that information ends up. Today cybercrime is a growing phenomenon on the planet and these criminals use precisely the information that Internet users enter to carry out identity theft, identity theft, robbery and crimes against intellectual property, among others.

Discussion

Can you talk about digital privacy in digital environments?

In the first place, the teaching methods have incorporated didactic tools that are supported by electronic devices and the Internet. Students observe, search, transform information, and conduct academic activities through various applications. Teachers have implemented digital books or texts, search portals, content storage and filing systems, e-portfolios, educational games, discussions in digital forums or chats, and other online collaboration tools. These teachers guide their students so that they discover themselves and can formulate their own ideas and make interconnections to achieve their goals (Amaya, Zúñiga, Salazar and Ávila, 2018).

In order to use these resources, teachers and students enter and entrust personal data and other products of our creativity to the sites and interfaces, ignoring the good or bad use they may make of them. In general, these applications and programs require the user to create an account and provide personal data such as name, age, day, month and year of birth, nickname, username, password, some others request photo, occupation and the Sites that are paid will have the information of the credit card and address for billing.

In addition, as Rallo and Martínez (2011) said, everyone, unconsciously, when searching or making a purchase on the Internet, leaves a mark on what interests us, which opens the possibility that strangers can know our activities and preferences. In other words, the Internet user leaves valuable traces of his identity that are translated into personal information, which comes to have a value that depends on the purposes of the person obtaining it.

Much of the information that we upload to these platforms is visible to all netizens; other data, despite not being exposed, can be hacked by computer technicians who gain unauthorized access to these applications and pages. In addition to the above, derived from cookies,[1] Information about habits and interests can be obtained, which can be used to the detriment of the Internet user (Norton, 2018). The consequent approach to privacy

[1] Una *cookie* es un archivo que contiene cantidades de datos que se envían entre un emisor, que es el servidor donde está alojada la página web, y un receptor, que es el navegador que se usa para visitar cualquier página web, con el objetivo de identificar el historial de actividad de los internautas, recabar direcciones y contraseñas del correo electrónico, teléfono y dirección, dirección de IP, el sistema operativo de nuestra computadora, el navegador que utilizamos y las páginas que hemos visitado anteriormente, entre otra información.

regarding the information that we enter in virtual environments arises, then: is there personal data in virtual environments and social networks?

It must be taken into account that the computer networks used by teachers and students are intangible places and that, although it is true that we cannot say that an interference in communications or in the sharing of personal information in the digital field is a violation of the privacy of the home, we can demand that the spaces or means through which our information is stored or shared be protected, just as people's homes are protected, since there is an expectation of privacy in a large number of operations and activities that we carry out on electronic sites. So, what must be considered for the legal norm to protect this information is the expectation of privacy that an individual has with respect to the places they enter, regardless of whether they are physical or virtual.

If someone enters without our consent and alters, makes use or seizes that data, it violates our right to privacy and, therefore, commits an illegal action that deserves to be sanctioned. Therefore, the guarantee of privacy in communications must cover the information shared and the activities carried out in these areas. Emails and personal information are included in this protection.

Specifically, the expectation of privacy of educational platforms is that to access the information, a service access provider, username and password are required, and because only the recipient is the one who has their password. personal, only he has the possibility to know its content. Now, there is the technical possibility of having access to the content, however, this does not imply having the legal possibility. And before the technical possibility of third parties to access our content, the right to the protection of our information must arise, which must be backed by both rigorous security mechanisms of the service providers or administrators and by legal regulations that penalize interference with our privacy.

Along the same lines, respect for the protection of information privacy should be extended to and should contemplate the "new" forms of communication through the Internet. In addition, it must be taken into consideration that what is protected is the private nature of the communications regardless of their content.

In addition, as previously stated, access to these Internet sites allows other companies to have access to our browsing, trends and preferences, and thus to our personal information. The link between the use of educational technology and the protection of information privacy and cybersecurity then arises.

According to a report published in 2016 by Norton, among the greatest risks that netizens take are:

- 34% do not protect the devices they have in their homes.
- 66% do not protect the Wi-Fi network in their homes.
- 61% entered financial information on the Internet when they were connected in public places.

Cyber or computer security is formed by those security measures or barriers both physical (including doors and locks) and logical (such as passwords) that users put in order to protect our computer assets and our information, considered as a protected legal asset.

The Norton report (2016) indicates that 76% of users know that they must protect their information, however, they share their passwords or carry out risky actions when using the Internet. According to their estimates, 35% of Internet users have at least one device without security controls, so they are left unprotected against the skills of cybercriminals.

Conclusions

The hypothesis of this work suggests that educational platforms do not provide security mechanisms. According to the exhaustive review of the chosen sites, 86% of them share user information with third parties and do not control the access that third parties may have to their users' information. All the platforms transfer responsibility for the use of the data to the user or are not responsible for the data processing. In addition, 68% of sites allow third parties to use the content of user data.

Regarding the knowledge that users have about cybersecurity, of a sample with a 95% confidence level, 58.1% of the surveyed population knows what it is about, while 41.9% does not know what it refers to. In addition to this, 40% of the surveyed students state that they do not properly close their session and 27.7% indicate that they accept the use of cookies on their devices.

Along the same lines, 62% of the surveyed sample does not know the treatment of educational platforms towards their personal data; only 38% say they know it. As if that were not enough, only 36.8% of the surveyed population knows the notices and privacy policies of educational platforms, the rest, 63.2%, do not know their content.

Finally, 40% of the students surveyed did not refer to the security methods used, since close to this same percentage are unaware of the issue of cybersecurity. Therefore, the persistent behavioral pattern in students is that they are not informed about the destination of the personal data that enter the Internet and they do not show interest in knowing and applying security mechanisms in their information.

Now, being the dependent variable the cyber security of the users of educational platforms, it was found that the frequency of use of their devices, the verification they make of the notices and privacy policies, as well as the knowledge of the handling of personal data on the part of electronic platforms, they have a direct relationship with the security of the information of the cybernauts. The latter constitute patterns of behavior that influence the safety of users, as they are related to the risky exposure of their information through the platforms. The reliability of the study was obtained using Cronbach's alpha coefficient. The coefficient obtained from the study was 0.77, making the study valid.

This study warns that there are no full security mechanisms on the part of internet service providers as regards the privacy of personal data and that this phenomenon imposes greater challenges on the user. Finally, governments must promote a culture of cybersecurity and promote actions to protect netizens by providing them with the necessary knowledge to protect the information they enter the network.

Future lines of research

Once it was discovered that the data of the users of the network did not enjoy full protection, a trail of questions opened up before us: who collects our information? Do they have the right to obtain it? How do they collect it? do with our information? and how do they use it? The study of the treatment of the data and traces that we leave on digital platforms can give rise to works that analyze and address these concerns.

References

Amaya, A., Zúñiga, E., Salazar, M., y Ávila, A. (2018). Empoderar a los profesores en su quehacer académico a través de certificaciones internacionales en competencias digitales. *Apertura. Revista de Innovación Educativa*, *10*(1), 104-115. Recuperado de http://www.scielo.org.mx/scielo.php?pid=S1665-61802018000100104&script=sci_arttext&tlng=pt.

Campo, A. (2006). Usos del coeficiente de alfa de Cronbach. *Biomédica*, *26*(4), 585-588.

Cataldi, Z. y Dominighini, C. (2015). La generación millennial y la educación superior. Los retos de un nuevo paradigma. Revista de Informática Educativa y Medios Audiovisuales, 12(19), 14-21.

Celina, H. y Campo, A. (2005). Aproximación al uso del coeficiente alfa de Cronbach. *Revista Colombiana de Psiquiatría*, *34*(4), 572-580.

Conde, S. y Boza, A. (2019). La educación del futuro: perspectiva del alumnado. Validación de una escala. *Apertura. Revista de Innovación Educativa*, *11*(2), 86-103. Recuperado de http://www.udgvirtual.udg.mx/apertura/index.php/apertura/article/view/1518.Crovi, D. (2010). Jóvenes, migraciones digitales y brecha tecnológica. *Revista Mexicana de Ciencias Políticas y Sociales*, *52*(209), 119-133.

Gallado, E., Marqués, L. y Bullen, M. (2014). Usos académicos y sociales de las tecnologías digitales del estudiante universitario de primer año. *Tendencias Pedagógicas*, *23*, 191-204. Recuperado de https://revistas.uam.es/tendenciaspedagogicas/article/view/2079.

Instituto Nacional de Estadística y Geografía [Inegi]. (2018). Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (Endutih) 2018. México: Instituto Nacional de Estadística y Geografía. Recuperado de https://www.inegi.org.mx/programas/dutih/2018/default.html.

López, M. C. (2007). Uso de las TIC en la educación superior de México. Un estudio de caso. *Apertura. Revista de Innovación Educativa*, *7*(7), 63-81. Recuperado de http://www.udgvirtual.udg.mx/apertura/index.php/apertura4/article/view/94/105.

Negroponte, N. (1995). *Being Digital*. United States: New York: Knopf.

Norton. (2016). *Norton Cyber Security*. *Insights Report*. United States: Norton. Retrieved from https://us.norton.com/cyber- security-insights.

Norton. (2018). Norton LifeLock Cyber Safety. Insights Report. United States: Norton. Retrieved from https://us.norton.com/cyber-security-insights-2018.

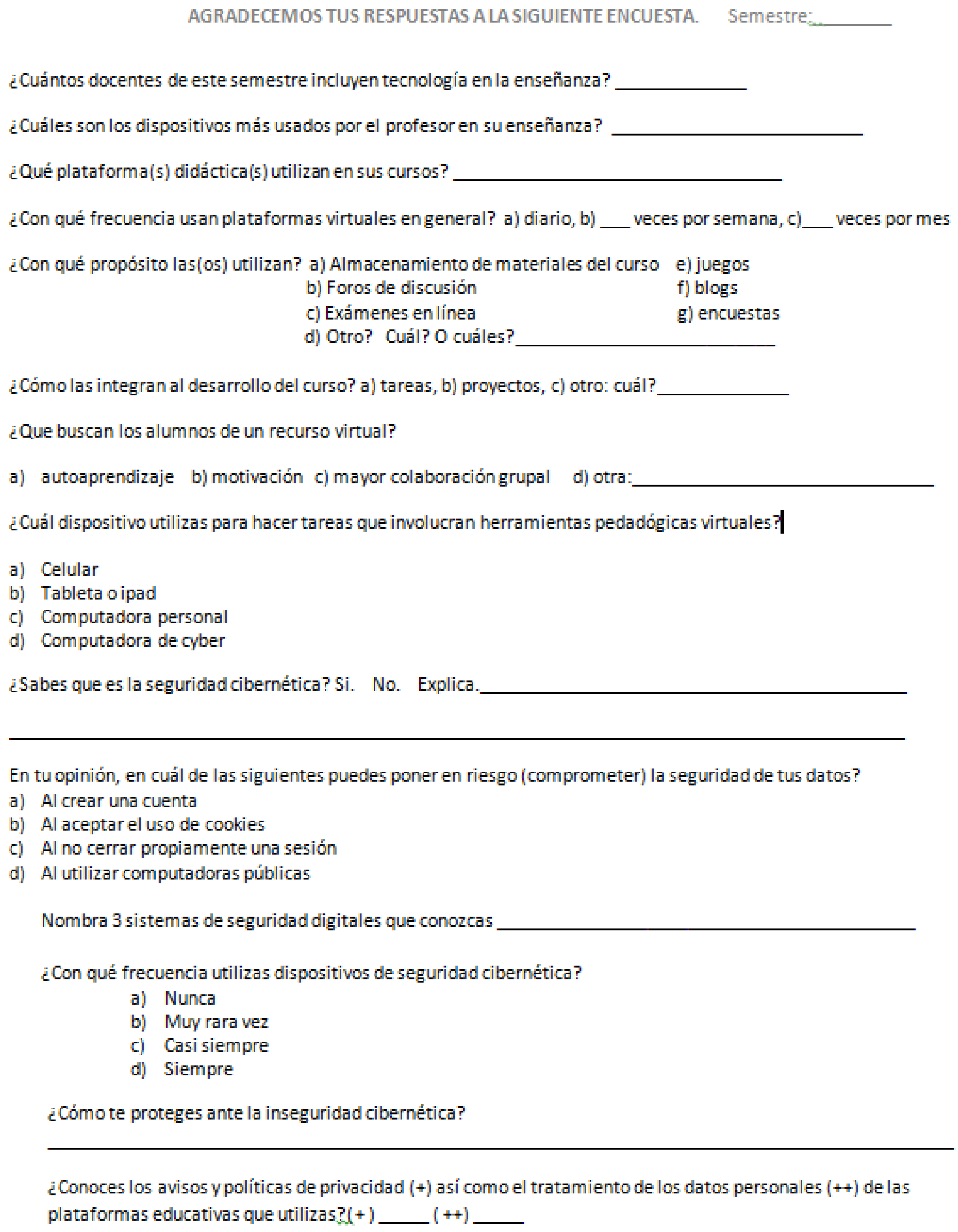
Quintero, J., Munévar, F. y Álvarez, D. (2009). Ambientes naturales y ambientes virtuales de aprendizaje. *Revista Colombiana de Educación*, (56), 12-37.

Rallo, A. y Martínez, R. (2011). Protección de datos personales y redes sociales: obligaciones para los medios de comunicación. *Quaderns del CAC*, *14*(2), 41-52. Recuperado https://www.cac.cat/sites/default/files/2019-01/Q37_Rallo_Martinez_ES.pdf.

Tapscott, D. (1998). *Growing Up Digital: The Rise of the Net Generation*. New York, United States: McGraw-Hill.

Anexo

Figura 7. Encuesta realizada a estudiantes de Criminología de la UASLP



AGRADECEMOS TUS RESPUESTAS A LA SIGUIENTE ENCUESTA.   Semestre:________

¿Cuántos docentes de este semestre incluyen tecnología en la enseñanza? ______________

¿Cuáles son los dispositivos más usados por el profesor en su enseñanza? __________________________

¿Qué plataforma(s) didáctica(s) utilizan en sus cursos? ___________________________________

¿Con qué frecuencia usan plataformas virtuales en general? a) diario, b) ___ veces por semana, c)___ veces por mes

¿Con qué propósito las(os) utilizan? a) Almacenamiento de materiales del curso   e) juegos
b) Foros de discusión   f) blogs
c) Exámenes en línea   g) encuestas
d) Otro? Cuál? O cuáles?___________________________

¿Cómo las integran al desarrollo del curso? a) tareas, b) proyectos, c) otro: cuál?______________

¿Que buscan los alumnos de un recurso virtual?

a) autoaprendizaje b) motivación c) mayor colaboración grupal d) otra:________________________________

¿Cuál dispositivo utilizas para hacer tareas que involucran herramientas pedagógicas virtuales?

a) Celular
b) Tableta o ipad
c) Computadora personal
d) Computadora de cyber

¿Sabes que es la seguridad cibernética? Si. No. Explica.____

____

En tu opinión, en cuál de las siguientes puedes poner en riesgo (comprometer) la seguridad de tus datos?
a) Al crear una cuenta
b) Al aceptar el uso de cookies
c) Al no cerrar propiamente una sesión
d) Al utilizar computadoras públicas

Nombra 3 sistemas de seguridad digitales que conozcas ____

¿Con qué frecuencia utilizas dispositivos de seguridad cibernética?
a) Nunca
b) Muy rara vez
c) Casi siempre
d) Siempre

¿Cómo te proteges ante la inseguridad cibernética?

____

¿Conoces los avisos y políticas de privacidad (+) así como el tratamiento de los datos personales (++) de las plataformas educativas que utilizas?(+) _____ (++) _____

Fuente: Elaboración propia