ISSN: 2230-9926

Available online at http://www.journalijdr.com

IJDR

International Journal of Development Research
Vol. 10, Issue, 04, pp. 35362-35369, April, 2020
https://doi.org/10.37118/ijdr.18701.04.2020

RESEARCH ARTICLE **OPEN ACCESS**

INFORMATION SECURITY: A SOCIOCULTURAL APPROACH TO ABOUT DIGITAL RESPONSIBILITY

[1]Kelson Pinheiro de Oliveira, [1]Bruno Pereira Gonçalves, [1]Ronei nunes ribeiro, [1]Jean Mark Lobo de Oliveira and [2,*]David Barbosa de Alencar

[1]Academic department, University Center FAMETRO, Amazon-Brazil
[2]Institute of Technology and Education Galileo of Amazon (ITEGAM), Brazil

ARTICLE INFO

Article History:
Received 19th January, 2020
Received in revised form
20th February, 2020
Accepted 13th March, 2020
Published online 30th April, 2020

Key Words:

Information security, Internet,
Virtual crimes, Digital maturity.

Corresponding author:
David Barbosa de Alencar

ABSTRACT

The digital environment is a place where procedures and processes are essential in the information security process. In this work, the sociocultural responsibility of the users in relation to the actions practiced within the virtual environment that may use high risk potential for use, integrity and availability of data will be addressed. For this, carry out a study with respect to the knowledge about the population about the importance of information security, as well as the knowledge of this group about sociocultural responsibility as an individual role in the use of digital media. Data collection was carried out through the application of semi-structured questionnaires, including questions aimed at knowledge and use of current information technologies. The selection of 112 respondents was carried out randomly, with no gender, age, education or social group standards. The answers were analyzed quantitatively and qualitatively through graphics and discussions about the needs and potential of the researched group. It is used as a basis, as norms of the ISO 27000 family, and a plan for confidentiality, integrity and availability (CID) is created, according to the public agreement of interest. With this research, there is no strong lack of knowledge and digital maturity and this scenario causes great losses for the general population, as it results in insecurity of the virtual environment for sharing data and information. Digital education deals with an emerging theme. The need to include an educational media as a strategy for users regarding the way of thinking and acting in the virtual environment contributes to the quality and security of the information contained in the virtual environment.

Citation: ***Kelson Pinheiro de Oliveira, Bruno Pereira Gonçalves, Ronei nunes ribeiro, Jean Mark Lobo de Oliveira and David Barbosa de Alencar.* 2020.** "Information security: a sociocultural approach to about digital responsibility*", International Journal of Development Research*, 10, (04), 35362-35369.

INTRODUCTION

Communication, as well as various segments of social, technological and economic interest, has undergone major changes over the years. The transformations resulting from the evolutionary processes of varied segments, walk with more speed than the psychic evolution of the human being, which causes great conflicts in the adaptation and use of the newly created tools (FRIEDMAN, 2018). In the case of information technology, the concern becomes even greater, as these tools, despite being often small and simple, have the potential to cause major disasters and disorders in the world in general, being able to interact and act passively or negatively. in politics, geopolitics, labor market, ethics and community (AUR, 2018). Information that used to take a long time to be disseminated today has an almost immediate spread, making transmission control a difficult task (FRIEDMAN, 2018; CURY *et al*., 2011). One cannot exclude or deny the benefits that technological advances have brought to humanity, however, the population's knowledge about communication tools must go hand in hand or as close to advances as possible, as it is now possible to see how much digital immaturity hinders advertising, facilitates online scams and puts confidentiality, integrity and availability of information at risk.

THEORETICAL REFERENCE

Definition and delimitation of Information and Communication Technologies (ICT) and media. The term technology comes from the Greek, where, according to Blanco and Silva (1993), technê, means art or craft, while logos, means study of something.

This automatically nostalgic term is reminiscent of old manual and slow processes that gradually gained agility and profitability from operating machines. Studying about information technologies (ICT), without first knowing at least a little about the historical evolution of this term, constitutes a hole in the construction of knowledge, where it is not possible to understand how and when the world started to live in an era of globalization in which geographical barriers and distance became unable to prevent the sharing of knowledge and information in a frighteningly fast way (CURY *et al*., 2011). Information technologies that existed before the 18th century, even slower and simpler compared to current advances, already had an impact on culture and social, economic, scientific and political perspectives. Introduced in Europe by Johann Gutemberg in the 14th century, letterpress printing, made from the transfer of ink over wooden arts or any material in high relief, to the sheet of paper, is considered one of the most important inventions in the history of ICTs. It is possible, based on this tool, to publish knowledge through books and then newspapers. The evolution of ICTs did not happen suddenly, first there were the first signs of electricity, then the need to spread knowledge and information and only after a few years, all these studies came together until the current advanced ICTs were obtained (GUIMARÃES, 2007; CURY *et al*., 2011).

Based on the knowledge about the evolution of ICTs, it is possible to better understand the boundaries of social media. For, the evolution of social media occurred along with the evolution of information technology (GEWEHR, 2016). Starting with the massive circulation of printed texts (books, newspapers, magazines) that already caused transformations in civilizations and contributed to major cultural, political and social changes. With the arrival of the most advanced means of communication during the eighteenth and nineteenth centuries (radios, televisions and later the internet), which already reached the population on a large scale, communication became something easy with never-before-thought amount of information and services . Today, a large part of the world population can quickly access any knowledge and products (CURY *et al*. 2011; KOBS, 2016). The emergence of Cyberculture, followed by the frightening advance of ICT, resulted in a tangle of information that could act positively and / or negatively in the dissemination of ideas and construction of critical thinking of human beings (LEVY, 1999). In this context, Alves (2009) reported that,

(...) Such technological advances provide transformations that are widely influencing education at all levels, opening the opportunity to integrate, enrich and expand the instructional materials, presenting new ways of interaction, so that the perspectives are of an increasing increase greater inclusion of information and communication technologies in the teaching-learning process (ALVES, 2009, p.13).

This scenario, where there has been an emergence of information dissemination, requires great challenges to maintain security within the virtual environment, requiring the inclusion of a more effective digital education, enabling the training of trained individuals with the knowledge of security tools and with critical look at the information received by the media. This being a great educational challenge, due to the need to rethink its fundamentals and innovate methods that assist in the training of these individuals (BÉVORT and BELLONI, 2009; ALVES, 2009). Media education as a strategy for disseminating knowledge and digital maturity.

According to Capurro (2014), the information acquired by technological means and interpreted individually, assumes an ontological meaning that has the purpose of "... giving shape to something material", which also interferes in the epistemological perspective that promotes knowledge communication to a person. This influence builds computerized learning, which can sometimes cause cognitive impairment to the individual. In view of this perspective, access to information assumes technical peculiarities and can be considered a highly manipulable tool. Because a single message can literally be interpreted in different ways (CAPURRO, 2014). It is not new to say that those born in the digital age or digital natives, have a greater emergence of information and interest in automated processes, which is a major challenge for most teachers used to resources where the return of knowledge is slower (BELLONI, 2009). However, Bévort and Belloni (2009), reports in their studies, on the importance of integrating media-education and integrated research into teacher training as a sine quan non condition. According to the authors, the change in posture caused by this integration involves effective practical and conceptual advances regarding the insertion of the media in education. Adaptive strategies for the inclusion of the information security approach. Some time ago, basic computer education was necessary in schools for students to learn how to use computers. However, nowadays, a large part of the population has access to these and other more current technology tools and, therefore, being able to use them with ease, the classes and computer labs in schools have been reduced. Varela (2017) reported in a publication to Época magazine, that 81% of public schools have a computer lab, but only 59% of these computers are used, and in most cases, for individual purposes of students (VARELA, 2017; NASCIMENTO, 2016; PINTO 2016).

Analyzing the needs of digital maturity and knowledge of the risks of the inconsistent use of these communication channels, it is necessary that adaptations occur in the teaching of computer science at school. Including as a curricular subject in order to guide students on the use and care that should be taken in the virtual environment. For this, it is necessary that teachers are trained and oriented to the use of strategies to reduce the digital “embryonic” in face of the consequences of the lack of security, in order to build an awareness that a safer virtual environment is made for the use of thought tools and actions adopted by the population. The growth of computer systems and facilities for accessing information has become even more accelerated with the dominance of cell phones and facilities for accessing the virtual environment, current researchers have reported that 71% of the population is connected. Therefore, studies on the use of these technologies should be treated as something mandatory in the school curriculum, because, together with the benefits of this great connectivity, there were many threats (LAVADO, 2019; RAMIRO, 2008). This increase in the number of users who do not have digital education, increases the amount of fraud and virtual scams. It is increasingly common for people to be bombarded with false advertisements and virtual promises that attract them to be able to scam and / or hack private data saved on cell phones. A study by Konduto, an online security company, highlighted that every five seconds, a company or individual, suffers some type of scam. In the banking sector, there is often a breach of confidentiality based on cloning of cards and passwords (O GLOBO, 2018).

Strategies to ensure confidentiality, integrity and availability of information (CID). All information presented in the virtual environment needs protection. The ISSO 27000 family addresses the rules for obtaining Information Security. These standards give rise to the Information Security Management System (ISMS), this system gave rise to the essential pillars in obtaining the security of digital data and electronic storage, which are the Confidentiality, Integrity and Availability (CID) of information, in addition to the basic principles of information security, reliability and authenticity. For Barros (2009) and Filho (2009), some CID elements are essential for Information Security and therefore, all users, from ordinary people to large companies, need to understand the individual role in protecting authenticity, responsibility, non-repudiation and reliability of information and, in addition, to know effective tools to fulfill these needs. The CID corresponds to three essential pillars for obtaining information security. Each pillar, constitutes a fundamental property that must be considered by each user. Confidentiality concerns the confidentiality of information, where the user must protect and take care so that his information is revealed only to authorized persons. Integrity, requires an accuracy of information. And availability, refers to information that is accessible and usable when authorized. Individual care with each of these criteria guarantees greater security within the virtual environment (PALMA, 2017).

Among the various security strategies determined by Information Technology (IT), there are those that are more specific to the security of business systems, as they offer more protection features for user control. These strategies are possible from the use of servers, which constitutes a resource storage network that are responsible for maintaining in the systems, applications necessary for the operation of various services on a network, being able to control electronic mails, databases, files of company information, DNS - "Domain Name System" (Name Resolution System), and / or any actions by all users, and these services can be accessed inside and outside the business environment through the internet (LIMA *et al*., 2019). As an example of these corporate security tools, we highlight the use of the DNS Server, which is used to access networks without the need to identify the IP. File server, which centralizes all company accessible information by department, which avoids file duplication, increases security and ease in making backups. E-mail server, which allows users to access the e-mail box within the corporate network. Backup server, which generates backup copies of important information of the company and its customers. Proxy server, which controls the pages visited by employees in a reservoir (cache), so that the most accessed pages are loaded directly by the server, which filters internet content and prevents the action of malicious software. In addition to firewall servers, which control everything that enters and leaves the network based on security policies selected by the IT team and virtualization, which consists of a technology that promotes scalability, reliability, agility, availability, high levels of performance and security centralized (Furtado and Rodrigues, 2013; Garlix, 2011; Microsoft, 2011; Golden and Scheffy, 2008, Kusnetzky, 2007; Alecrim, 2005, Lopes 1997). Although the use of servers is a very effective security strategy, it does not consist of an application accessible to ordinary users, as these are complex procedures that require professional knowledge. Therefore, in this work, the study of accessible and effective strategies for the security of information of ordinary users will be carried out. As well as the creation of an ICD based on ISO 27000 based on studies of the main needs related to information security demonstrated in this research.

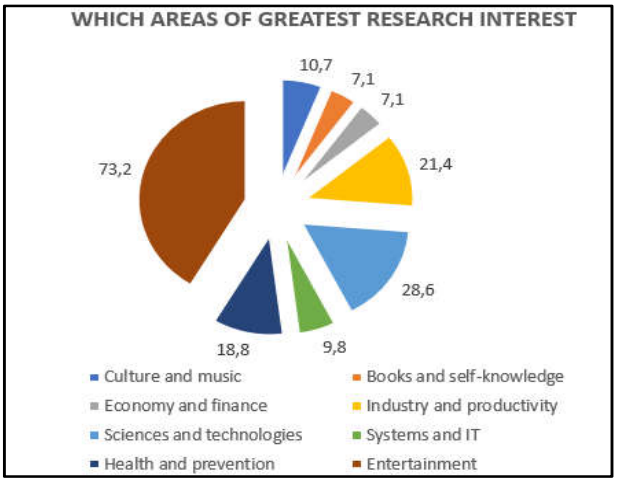
MATERIALS AND METHODS

Materials and data collection: The research carried out followed methodological characteristics that apply to the exploratory style, as it allows the researcher to become more familiar with the topic addressed, before starting a socio-cultural discussion about digital responsibility. According to Gil (2007), exploratory research provides greater familiarity with the problem, in order to make it more explicit or to build hypotheses. In this sense, the interview was adopted in this research, based on a semi-structured questionnaire that allowed to obtain the main data for the discussions in this article. Some interviews took place through the Whatsapp application, due to the need for social isolation in the current scenario in Brazil.
The questionnaires used were randomly distributed to 112 people. In some cases, the author endeavored for the interviewees to have different characteristics regarding age, education, profession, in order to obtain a greater universe of profiles to be analyzed. The questionnaires were analyzed individually and in some cases, where identical responses occurred among respondents with similar profiles, significant discussions for the present study were considered. The questions used in the questionnaire followed the central idea of the present study, which is summarized in the research when actions and understanding of the main needs of the interviewees regarding information security. The results were analyzed quantitatively and qualitatively, using graphs and spreadsheets.

RESULTS AND DISCURSION

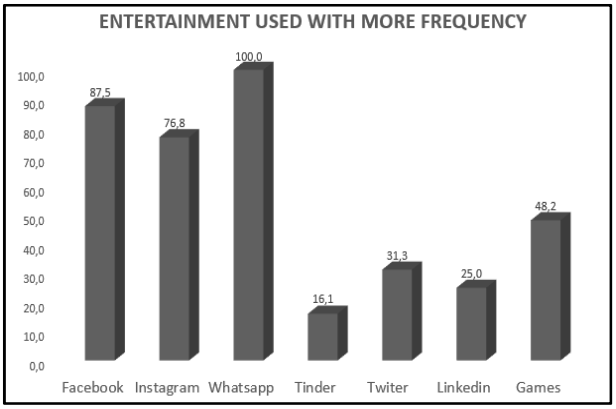
The work could count on 112 interviewees of different profiles and belonging to different social groups. This acted positively in the characteristic of this research, as it was found that digital maturity can occur regardless of gender, age, education or social group. To fulfill the objectives of this research, the interview was organized in order to get to know a little about the profile of the researched group, paying attention initially to the use of digital tools, affinities with social networks, conduct in virtual environments and use of functional applications, until you get into issues regarding security and protection tools. In general, all respondents had access to the virtual environment. Most of them reported as the first option the frequent use of this technology for entertainment (71.2%), which is related to the use of social networking applications and games.

The second option is to use it for research, as shown in Figure 1. Among the entertainment options, it was possible to verify that Whatsapp is the most used application by the interviewees, appearing with 100% use, followed by Facebook (87.5%) and Instagram (76.8%), as shown in figure 2. It was noted in the study of the questionnaires that the use of the other applications highlighted in the image is characteristic of specific groups. LinkedIn (25%), for example, which consists of a platform for professional integrations, came to be classified by some respondents as the second most used platform, behind Whatsaap only. The other platforms, Tinder (16.1%) and Twiter (31.3%), proved to be used by a more specific audience, who reported seeking more characteristic entertainment. The use of these platforms is always an invitation to the unknown.



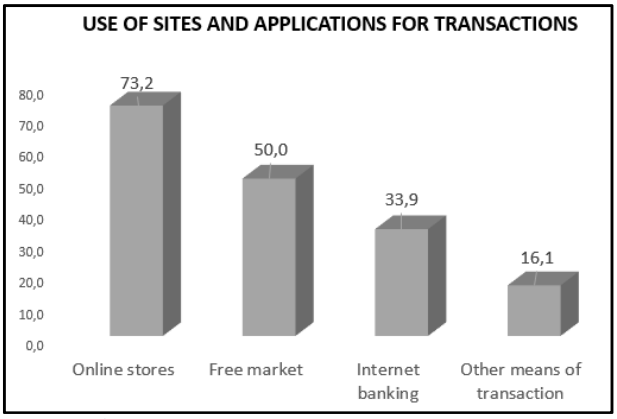
Source: Authors, (2020)

Fig. 1. Areas of greatest interest and use of virtual media by respondents



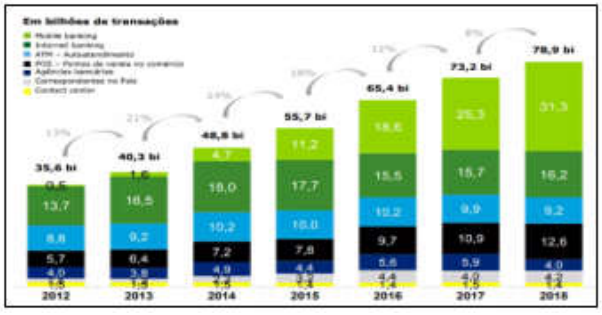
Source: Authors, (2020)

Fig. 2. Main entertainment applications used by respondents.



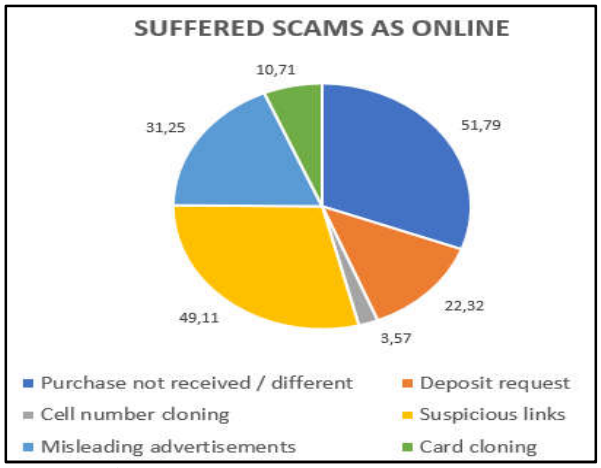
Source: Authors, (2020)

Fig. 3. Sites and applications most cited by respondents regarding online credit card transactions



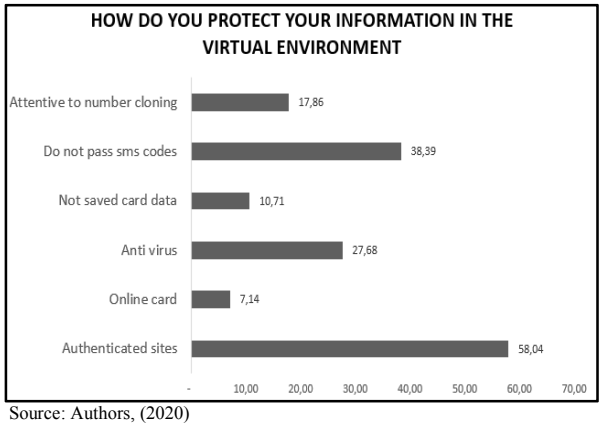
Source: Authors, (2020).

Fig. 4. Increase in bank transactions carried out in 2012 and 2018



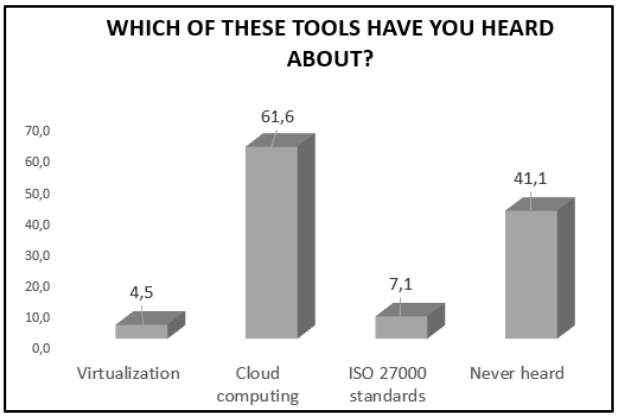
Source: Authors, (2020)

Fig. 5. Percentage of the main online scams cited by respondents



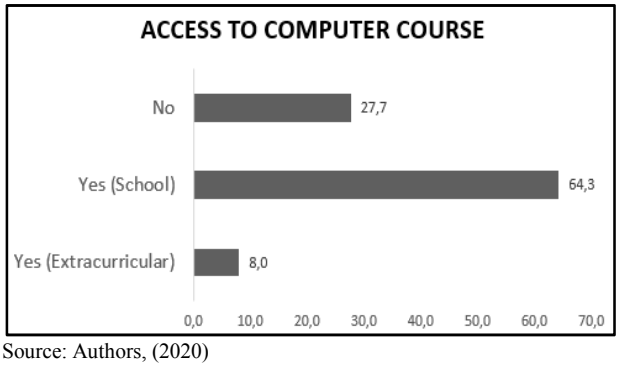
Source: Authors, (2020)

Fig.6. Security strategies practiced by the interviewees.



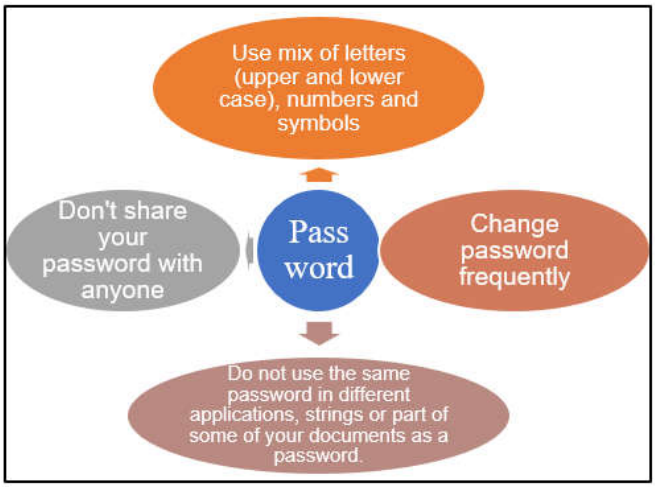
Source: Authors, (2020).

Fig. 7. Percentage of respondents who have already taken a computer course over their lives



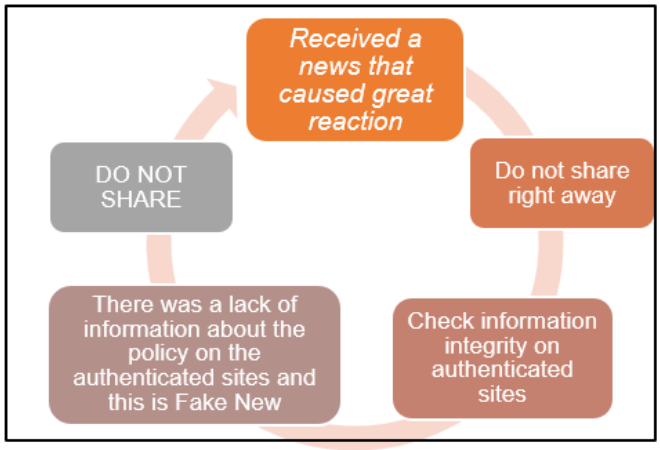
Source: Authors, (2020)

Fig. 8. Interviewees' knowledge of current technological tools



Source: Authors, (2020).

Fig. 9. Strategies to guarantee the confidentiality of passwords for ordinary users



Source: Authors, (2020).

Fig. 10. Cycle of actions that ensure the integrity of the user when receiving information, news, promotion, before sharing

Messages with false information, malicious links containing cyber criminal actions and a shower of advertisements that are directly related to the user's main searches, are some of the main ways of contact with cyber crimes (MAUES *et al*., 2018). In the virtual environment there is an immense amount of data and, according to Marquesone (2017), it is possible to gain access to this volume and variety of information through Big Data, where the information is collected in great volume, variety and speed. For companies, this resource is of great importance, as it is possible to know the profile and the need of each user from a few clicks that they make while using the virtual environment, thus being able to cast small baits to attract it in their favor. . But this tool also represents a security risk, since not only secure companies have access to this information, but also digital criminals who use this mechanism to commit illegal acts. Another issue of great relevance to information security that was raised in this research, concerns the use of the virtual environment to carry out credit card transactions (Figure 4). Among those interviewed, 84% stated that they had already carried out transactions or any type of credit card purchase over the internet. Most of the users present in this research, mentioned that purchases in online stores have been the main form of use of credit cards in the digital environment, with the free market leading the search for attraction of consumers, with 50% of users who constantly use the channel. 73% of users said they also use other online stores. 33% of users use internet banking for transactions and payments and still have a percentage of 16% of respondents who use other applications to carry out transactions, such as Picpay. According to the Brazilian Federation of Banks (FEBRABAN), in 2018 the number of bank transactions carried out using cell phones (Mobile banking) increased by approximately 42% from 2015 to 2018 (figure 4). This popularization of credit card transactions over the internet tends to proliferate the incidence of card fraud. Roca and Jakitas (2018), pointed out that between January and August 2018, over the internet, there were more than 920 thousand scams aimed at stealing consumers' financial data for cloning credit cards. This corresponds to 3.6 frauds per minute. One of the reasons that can lead users to be less careful when buying online, is the certainty that they are insured by the card administrator in cases of fraud. Thus, even with the numerous advertisements encouraging the responsible use of credit cards, many users fail to adhere to simple security strategies, since the only consequence that can affect them is the cancellation and receipt of a new card. In order to find out the occurrence of cases of fraud or attempted scams experienced by respondents, the result of the survey was almost unanimous, 98% of respondents have already suffered scams and / or went through some situation considered suspicious. In figure 5, it is possible to verify that most cases of scams suffered by the interviewees, occurred during online purchases. 51.8% of respondents have already purchased a product and have not received or received a product other than that advertised. Second, 49.1% reported having clicked on a suspicious link received via email or Whatsapp. In third place in this research, there is the deposit request (22.3%), which in most cases is the result of cloning the cell number of a contact. Credit card cloning was the scam that appeared in the lowest percentage in the survey, 3.6% of respondents. However, FEBRABAN states that this number has increased consecutively to the online use of the credit card. These data show that there is a great need to work on digital education.

As mentioned in the methods of this work, it was decided to choose a heterogeneous group, with people of different schooling, age, social class, interests in the digital environment, profession. And it was possible to notice that everyone, at some point in the research, demonstrated the need to know and develop individual security methods in the virtual environment. As an example of this need, it stands out that both the person who had the cell phone number cloned and the person who was the victim of the deposit request of a cloned contact, could have prevented these crimes if they had knowledge about the strategic security tools . Being a victim or practicing an illegal act within the virtual environment is not only related to issues that cause material damage to the user, but also issues that cause moral or psychological damage to someone (NEVES, 2019). This statement concerns civil liability on social networks. Relating within a society involves conflicts and the same occurs in the virtual environment, where there are omissions, accusations, and a special focus on this work will be given to Fake News. The sharing of news without previous confirmation of veracity is one of the major problems that grew along with the popularization of the virtual environment (MARTINS, 2018). The belief in fake news is a sociocultural phenomenon that clearly demonstrates a flaw in digital education, something that needs to be corrected as soon as possible. In the present study, 83.3% of respondents said they did not share false news. These results can be reliable for this

research universe, however, in the current scenario, which has been moving the world with the corona virus pandemic (COVID19), for example, it shows that there is still a large portion of the population that shares information before confirm the veracity. This is an issue that has been discussed a lot nowadays and, although it is something still quite committed, users tend to deny this practice, either out of naivety or out of shame for knowing that they are not correct in practicing these actions. The psychiatrist Claudio Martins, in an interview with the British Broadcasting Corporation (BBC), compared the sharing of Fake News to the use of narcotics, where people act consciously of the consequences and in that act, they experience feelings of well-being similar to the use of drugs. So-called rumors have always been present in society. Renard (2007) points out that the rumor can be distinguished as unverified information or as false information. These actions cause great damage to the reliability of the virtual environment, requiring the user to know how to filter and investigate any news that circulates in this medium. In a subjective question of the research referring to the scams commonly occurred in the digital media and how much it affected the interviewed users, it was found that a large part (88.9%), had a feeling of insecurity during the use of the virtual medium. The incidence of links with viruses, failure to receive or receive products different from what they bought on unreliable sites, fake promotions, cloned cards, fake news, password theft, account loss in applications, were the main digital crimes cited in the survey. Among respondents, it was noted that 12.1% did not feel threatened by the current attacks. Of this group, 78% reported that they are very careful and follow all possible security strategies, such as not clicking on links or news before investigating the veracity and use of online cards. The others, who reported not feeling threatened by online attacks, demonstrate a little lack of knowledge about what can be considered criminal actions in the virtual environment. In figure 6, it is possible to verify the main care cited by the interviewees regarding information security in virtual environments. In this matter, the interviewees could check one or more alternatives that included security actions developed by them in the virtual environment.

Thus, 100% of users marked some type of safe action. 58% of them reported accessing only authenticated sites. 38.4% said they were on the lookout for confirmation password requests. 27% cited the use of antivirus. Other strategies mentioned appeared with a lower percentage, mainly those related to the use of credit cards and personal data. It was possible to realize that there is knowledge about the possibilities of protecting oneself from online scams, however, even so, in the researched group, a large percentage of people have already been victims of some fraud. This result supposes situations that have already been discussed throughout this study, many people are lacking in media education and many others do not practice safe acts for convenience. Lack of knowledge, as seen in this universe of research, clearly demonstrates a flaw in virtual education. In some cases, it can be classified as a kind of digital illiteracy, according to studies by the Brazilian Psychiatric Association. In other cases, it is understood that there is knowledge and at the same time a lack of awareness of the responsibility for taking safe actions. It is seen that people are able to move around in the virtual environment, but they do not recognize the risks they are subject to, making this digital “embryonic” a socioeconomic phenomenon that needs attention. According to Capurro (2014), the information acquired by technological means and interpreted individually, assumes an ontological meaning that has the purpose of "... giving shape to something material", which also interferes in the epistemological perspective that promotes knowledge communication to a person. This influence builds computerized learning, which in turn can cause cognitive impairment to the individual. In view of this perspective, access to information assumes technical peculiarities and can be considered a highly manipulable tool. Because a single message can literally be interpreted in different ways (CAPURRO, 2014). Among the questions asked to the interviewees, it was sought to know how many of them were taking or have taken a computer course. The result showed that 27.7% of respondents never had access to a computer course. 55.4% answered that they had attended a regular school and 8% reported having taken an extracurricular course, as shown. The qualitative analysis of the questionnaires made it possible to contact, that the interviewees who presented more digital awareness, are part of the groups that at some point in their lives had access to computer education. Which leads us to think about the real importance of incentives for teaching computer science in schools. As seen, a total of 58.9% of respondents answered that they had already heard about the words mentioned in the question, with 4.5% marking virtualization, 61.6% marking cloud computing and 7.1% said they have already having heard about the ISO 27000 standards. However, when questioning the qualitative discussion of this research, the respondents' response was unanimous when reporting that although they had heard about the terms at some point, they never used it and so they did not know how to highlight the tool features. Thus showing the urgency of computer education. Among the objectives of this study, it was proposed to set up a support plan that addressed the needs of this target audience. Thinking about this scenario, in the following steps of this work, the principles of confidentiality, integrity and availability (CID) provided for in ISO 27000 were used to present security strategies that are easy to act for ordinary users. Information security criteria directed to the common user.

As seen throughout this study, there are several small issues that need to be considered before setting up an ICD that addresses the needs of the target audience in question. It is a mixed group, aged between 15 and 60 years old, students of various levels, with a career in different areas. In common, the use of the virtual environment for entertainment and shopping stands out. Therefore, in this work, the intention is to reach the individual user, who uses the online environment daily for distraction and solving day-to-day facilities. In this sense, the scheme to be assembled next, will include tools and actions that are easy to handle and that are effective to ensure greater security in the main channels used by these users. Each pillar (Confidentiality, Integrity, availability), corresponds to a central need that will take the user to the safe act. Both entities, as well as the private user, the role of taking care to ensure that data is protected is individual, therefore, the importance of knowing from small security actions is affirmed. The following 9 steps will be organized in tables and / or schemes containing a specific subject and security strategies that can be adopted. The assembly of the CID will follow specific strategies that a common user can adopt in order to guarantee each of the pillars of security. Starting with the pillar of Confidentiality, the barrier that exists between individual information within the virtual environment is the effectiveness of access control, which can occur through the use of secure passwords, whether for initial access of the cell phone, notebooks and / or for access to websites, apps and emails. In figure 9, you can see some ways to protect your confidentiality within the virtual

environment. In addition to the use and maintenance of secure passwords, confidentiality involves other strategies that are effective for user security, such as, for example, two-factor authentication or two-step confirmation that are strategies available in various applications and prevent unauthorized access to accounts, even when the password is compromised. This function is available on platforms with record users, such as whatsapp, facebook. Another easily accessible information confidentiality strategy is the use of an online credit card. This update in the banking system tends to reduce the incidence of card cloning and, consequently, the risk of fraud. It is a benefit provided at no additional cost and that accompanies the same physical card bill. The use of antivirus, verification of authenticity of websites, the non-sharing of bank details and individual identification document, attention to e-mail and suspicious messages, which offer advantages, which charge debts or anything else that surprises you, are also secure strategies to be practiced in order to maintain the confidentiality of your data. The second criteria scheme to be presented refers to Information Integrity. This pillar is the role of transferring information correctly and loyally. In the case of ordinary users, where, for the most part, they are recipients of information, promotions and events brought by companies, Fake News comes into the discussion, a fact that occurs when information is tampered with or invented. It is often not an easy task to identify a fake news, however, in most cases, a rumor can be suspected when the reader is surprised by the news, this is the main intention of cyber criminals when launching a fake publication . This will facilitate the dissemination or, the user's click. The chain of evil caused by the rumor can be broken as soon as the information is confirmed on secure websites. In Figure 10, you can find the cycle of actions that must be followed to identify a fake News and guarantee the integrity of the information received before sharing.

The third and last pillar to be discussed with usual strategies for the target audience of this research, is the availability of information. This criterion is related to the need and the possibility for information to be accessed whenever necessary and safely. It is common to need to archive documents, card photos, personal information, so that they are easily accessible when necessary. Therefore, part of the users tend to photograph these documents, open and send them by e-mail and keep this data on the mobile device, which corresponds to a great risk to the security of this information. Since, it may happen to lose the cell phone, have the notebook stolen and thus, all information will be available for digital criminals to act. In addition, the action of a virus is able to access these environments and make use of the archived data. Another issue, which leads to thinking about the practical side of availability and that no electronic device will last forever and whenever it is necessary to change it, needs to do all the data transfer, this is not practical for the current technological evolution. Therefore, as a strategy to obtain this availability of information safely, you can use cloud storage, in English as the cloud is also known. The advantage of the cloud is the ability to keep all your files, photos, videos and everything you need to keep, intact and safe. With this feature, even if your electronic device is stolen, lost or broken, you will be able to access your information easily, on any other device on which you release access. This tool is available free of charge, however, to obtain more space, it is available on the market. As seen, information is a valuable asset for the user. Each pillar of information security includes necessary actions and security benefits. Without confidentiality, personal data will leak, which can cause major problems for the user and even his community of contacts. Failure in integrity strategies, the user loses credibility, in addition to contributing to the spread of false information that undermines the reliability of the digital environment. And without availability, the user can lose important files and unforgettable records. Thus, information security must be taken more seriously, in order to build a safe and meaningful environment for humanity.

Final Considerations

The great repercussions caused by the cases of cyber crimes, these crimes being the result of financial and moral damages to users, attracted attention to study the importance of information security awareness of ordinary users. In this work, it was possible to notice that there is an educational deficiency regarding good information security practices. It was noted that respondents constantly suffer from bombings of fake news, card cloning, attempted fraud, scams, among other problems caused by the lack of malice and knowledge about information protection strategies within the virtual environment. During the study of this topic, it was noted that there is a great concern in dealing with information security within business environments, highlighting the implementation of ISO27000 as a differential with regard to security. However, when it comes to a strategy to ensure the safety of the general public, little is found. With the great space that Information Technologies (ICTs) have reached over the years, becoming a world trend of great cultural, social and political power, it is necessary that great transformations occur in the way of acting against these technologies, being this possible from the media education as an essential subject in the school curriculum.

ACKNOWLEDGMENT

Above all, I thank God, allowing me to get here, even in the face of all difficulties, blessing me with his light of hope. To my parents and my wife, for their love, encouragement and unconditional support. They being my pillars and greatest motivators. FAMETRO and its faculty, which provided an educational environment to finally reach that point. To the advisor Bruno Pereira Gonçalves, for his dedication and support in the development of the article, for his corrections and incentives. And to all those who directly or indirectly, mainly friends, took part in this endeavor, contributing to my training, my thanks.

REFERENCES

Alecrim, Emerson. Básico sobre DNS (Domain Name System). Infowester, 2005. Disponível em: < http://www. infowester.com/dns.php>. Acesso em 30 de janeiro de 2012 ABEPRO, 2008. Disponível em: <http://www. abepro.org.br/biblioteca/enegep2008_TN_STP_077_543_ 11709.pdf>. Acesso em 20 de Março de 2020.

Alves, T. A da S. Tecnologias de Informação e Comunicação (TIC) nas escolas: da idealização à realidade. Instituto de Ciência da Educação. Dissertação. Universidade Lusófona de Humanidades e Tecnologias. Lisboa, 2009. Disponível em http://recil.grupolusofona.pt/bitstream/handle/ 10437/1156/Taises%20Araujo%20-%20versao%20final% 20da%20dissertacao.pdf?sequence=1. Acesso em Março de 2020.

Bastos, A.; Caubit, R. ISO 27001 e 27002 - Uma visão prática. Porto Alegre, RS: Módulo Education Center, 2009. 257p.

Belloni, M. L. O que é mídia Educação. 3º Edição. Rev. Campinas São Paulo. Coleção polemicas do nosso tempo, p.78, 2009.

Bévort, E.; Belloni, M. L. Mídia-educação: Conceitos, história e perspectivas. Educ. Soc., campinas, vol. 30, n. 109, p. 1081-1102, set./dez. 2009

Blanco, E.; Silva, B. D. Tecnologia Educativa em Portugal: conceito, origens, evolução, áreas de intervenção e investigação. Revista Portuguesa de Educação, Portugal 1993.

Capurro, R.; Hjorland, B. O conceito de informação. Perspectivas em Ciência da Informação, Belo Horizonte, v. 12, n. 1, p. 148-207, 2007. Disponível em: <https://doi.org/10.1590/S1413-99362007000100012>. Acesso em 18 de Março de 2020.

Cury, L.; Capobianco, L. Princípio da história das tecnologias da informação e comunicação Grandes Invenções. VII Encontro Nacional da história da mídia, Unicentro, Guarapuara, PR, 2011.

Friedman, Thomas. "A tecnologia está evoluindo mais rápido do que a capacidade humana". Época negócios. Colunista do The New York times em entrevista no Amcham, SP. Disponível em https://epocanegocios.globo.com/Tecnologia/noticia/2018/03/tecnologia-esta-evoluindo-mais-rapido-do-que-capacidade-humana-diz-friedman.html. Acesso em 19 de Março de 2020.

Furtado, Bruno Mendonça; RODRIGUES, Rômulo Eduardo Sirqueira. Proposta de política de segurança da informação física e lógica para centelha tecnologia da informação. Trabalho de conclusão de curso. Faculdades Promove de Brasília. Guará, 2013. Disponível em http://nippromove.hospedagemdesites.ws/anais_simposio/arquivos_up/documentos/artigos/0dbc75be384ecb72b4a5906783bd139b.pdf. Acesso em 25 de Março de 2020.

Gewehr, D. Tecnologias digitais de informação e comunicação (TDICS) na escola e em ambientes não escolares. Centro universitário Univates. Programa de Pós graduação Stricto Sensu. Mestrado. Lajeado, 2016. Disponível em https://www.univates.br/bdu/bitstream/10737/1576/1/2016DiogenesGewehr.pdf. Acesso em 10 de Março de 2020.

Gil, A. C. Como elaborar projetos de pesquisa. 4. ed. São Paulo: Atlas, 2007. Disponível em http://home.ufam.edu.br/salomao/Tecnicas%20de%20Pesquisa%20em%20Economia/Textos%20de%20apoio/GIL,%20Antonio%20Carlos%20-%20Como%20elaborar%20projetos%20de%20pesquisa.pdf. Acesso em 03 de Abril de 2020.

Golden, Bernard; Scheffy, Clark. Virtualization for Dummies, Sun AMD Special Edition. Indianapolis: Wiley Publishing INC, 2008.

Guimarães, A. de M.; RIBEIRO, A. M. Introdução às tecnologias da informação e da comunicação: tecnologia da informação e da comunicação. Belo Horizonte. Editora UFMG, 2007.

https://economia.uol.com.br/noticias/estadao-conteudo/2018/09/25/fraudes-em-cartao-de-credito-ja-passam-de-920-mil-no-pais-desde-o-inicio-do-ano.htm. Acesso em Abril de 2020.

Kobs, Fabio Fernando; CASAGRANDE JUNIOR, Eloy Fassi. O papel das tecnologias digitais na educação: perspectivas para além dos muros da escola. Rev. Cienc. Educ., Americana, ano XVIII, n. 34, p. 41-73, jan./jun. 2016.

Lavado, Thiago. Uso da internet no Brasil cresce, e 70% da população está conectada. G1 Economia. Disponível em https://g1.globo.com/economia/tecnologia/noticia/2019/08/28/uso-da-internet-no-brasil-cresce-e-70percent-da-populacao-esta-conectada.ghtml. Acesso em 19 de Março de 2019.

Lévy, P. Traduzido por Costa, C. I. da. Cibercultura. São Paulo. Edição 34, coleção TRANS, p. 264, 1999.

Lopes, Raquel. Firewall, Boletim bimestral sobre tecnologia de redes publicado pela Rede Nacional de Ensino e Pesquisa. 1997. Disponível em: <http://www.rnp.br/ newsgen/9708/n3-1.html>. Acesso em 25 de Março de 2020.

Marquesone, Rosangela. Big data: O desafio das empresas e profissionais do mercado. Palestra para Universidade de São Paulo, 2017. Disponível em http://paineira.usp.br/lassu/wp-content/uploads/2017/01/2017.02.07-palestra_rosangela_bigdata.pdf. Acesso em 30 de março de 2020.

Maues, Gustavo Brandão Koury; DUARTE, Kaique Campos; CARDOSO, Wladirson Ronny da Silva; CRIMES VIRTUAIS: Uma análise sobre a adequação da legislação penal brasileira. Revista Científica da FASETE 2018.1. Disponível em https://www.unirios.edu.br/revistarios/media/revistas/2018/18/crimes_virtuais.pdf. Acesso em 29 de Merço de 2020.

Medeiros, Henrique. 92 % dos Brasileiros possuem ou usam smartphones com frequência. Mobile Time, 2019. Disponível em https://www.mobiletime.com.br/ noticias/18/10/2018/92-dos-brasileiros-possuem-ou-usam-smartphones-com-frequencia/ Acesso em 08 de Março de 2020.

NASCIMENTO, D. M. A abordagem Sociocultural da informação. Informação e Sociedade. João Pessoas. v.16, n.2, p.25-35, jul./dez. 2006. Disponível em https://www.brapci.inf.br/_repositorio/2010/11/pdf_fc196bfb47_0012820.pdf. Acesso em 20 de Março de 2020.

PALMA, Fernando. CID: Confidencialidade, Integridade e Disponibilidade. Critérios da informação pela perspectiva da segurança. Portal GSTI. Disponível em https://www.portalgsti.com.br/2016/11/cid-confidencialidade-integridade-e-disponibilidade.html. Acesso em Abril de 2020.

PINTO, K. L. J. Desafios da formação inicial e as novas tecnologias na educação: grupo focal com licenciandos de Minas Gerais. 3° congresso Nacional de Educação. Instituto Federal do Rio Grande do Sul, 2016. Disponível em http://www.editorarealize.com.br/revistas/conedu/trabalhos/TRABALHO_EV056_MD1_SA4_ID8789_04082016165409.pdf. Acesso em 24 de Março de 2020.

ROCA, Gabriel; JAKITAS, Renato. Fraudes em cartões de crédito já passaram de 920 mil desde o início do ano. UOL Economia. 2018. Disponível em

Servidores e Redes de Computadores. Disponível em: <http://www.garlix.com.br/index.php?option=com_content&view=article&id=69&Itemid=96 >. Acesso em 20 de Março de 2020

Souza, Felipe. BBC BRASIL - British Broadcasting Corporation. 'É como usar drogas': por que as pessoas acreditam e compartilham notícias falsas? Publicado em 2018. Disponível em https://www.bbc.com/ portuguese/brasil-45767478. Acesso em Abril de 2020.

****