Journal of Information Systems and Technology Management – Jistem USP
Vol. 15, 2018, e201815005
ISSN online: 1807-1775
DOI: 10.4301/S1807-1775201815005

INFORMATION SECURITY MANAGEMENT PRACTICES: STUDY OF THE INFLUENCING FACTORS IN A BRAZILIAN AIR FORCE INSTITUTION

Rogério dos Santos Ferreira[1] http://orcid.org/0000-0001-9254-0722
Rodrigo Franklin Frogeri[2] http://orcid.org/0000-0002-7545-7529
Alessandra Brum Coelho[1] http://orcid.org/0000-0003-4778-8707
Fabrício Pelloso Piurcosky[2] http://orcid.org/0000-0001-5458-5129

[1]Diretoria de Tecnologia da Informação da Aeronáutica, Rio de Janeiro, RJ, Brazil

[2]Centro Universitário do Sul de Minas - UNISMG, Varginha, MG, Brazil

ABSTRACT

This article aims at analyzing the factors which influence the staff of the Brazilian Air Force Information Technology Board – DTI in relation to the understanding of the application of the Information Security Management practices. This attempt was based on the hypothetical-deductive method and, as to its objective, it was descriptive in nature. As to the approach of the research problem, it was quantitative in nature. In order to achieve the proposed objective, an adaptation of the Theoretical Technology Acceptance Model – TAM, which allowed the analysis of the relation between sociodemographic profile, perceived ease of use, perceived usefulness, attitude and behavior of the users, and the level of understanding of the Information Security practices. The survey was conducted with 59 military servants and civilians which are part of the Brazilian Air Force Information Technology Board, to whom a questionnaire was applied, submitted and approved by the Committee of Ethics in Research (CAAE: 62636016.7.0000.5111), which was based on the precepts of ISO/IEC 27001 (2013) and 27002, which deal, respectively, with the Information Security Management system and with the code of practice for Information Security controls. Once the data were gathered, they were tabulated and statistically analyzed, which enabled the demonstration of the influence of sociodemographic and behavioral factors and of the precepts of the TAM in the perception of the Information Security practices by the DTI staff.

Keywords: Information Security, Management, ISO/IEC 27001, ISO/IEC 27002, Technology Acceptance Model – TAM, Brazilian Air Force Information Technology Board.

Manuscript first received: 2017/10/11. Manuscript accepted: 2018/05/03
Address for correspondence:
Rogério dos Santos Ferreira, Diretoria de Tecnologia da Informação da Aeronáutica, Rio de Janeiro, RJ, Brazil
E-mail: rogerioferreira.dsf@gmail.com
Rodrigo Franklin Frogeri, Centro Universitário do Sul de Minas - UNISMG, Varginha, MG, Brazil
E-mail: rodrigoff@unis.edu.br
Alessandra Brum Coelho, Diretoria de Tecnologia da Informação da Aeronáutica, Rio de Janeiro, RJ, Brazil
E-mail: alebcoelho@yahoo.com.br
Fabrício Pelloso Piurcosky, Centro Universitário do Sul de Minas - UNISMG, Varginha, MG, Brazil
E-mail: fabricio@unis.edu.br

CC BY

CONTEXTUALIZATION

The demand for the immediate access to information in the corporate environment has considerably increased in the last years, and the professionals of the information era are increasingly more demanding as to the availability and speed with which they may access their systems, by means of the most varied technological devices.

According to Sêmola (2014), we live in the era of the big data, in which huge amounts of information are generated, stored, manipulated, and shared all the time, among the most diverse kinds of organizations. The access channels to the Internet are increasingly faster and more accessible and the computational power is no longer a problem for most companies.

The scenario with which the Information and Communications Technology – ICT managers deal is very different from the scenario of a few years ago. In a short period, the information stopped being dealt with in a centralized and little automated manner, and became a part of the business strategy of the organizations. The data processing centers became obsolete, giving up space to the corporate networks, which provide more performance and speed to the information access, and which, on their turn, have become the main channel of distribution of information through the Internet, integrating the organization to the other elements of the chain of production, such as suppliers, partners, clients, and government (SÊMOLA, 2014).

This scenario tends to become even more complex, as it can be observed in the study commissioned by the Chamber of Technology Strategy and prepared jointly with PricewaterhouseCoopers LLP (BRASIL, 2010), of the United Kingdom, when the main trends which will conform the future of information security by the year 2020 were mentioned, among which it is important to emphasize the revolution of the infrastructure and the data explosion.

According to the study, the infrastructure revolution will occur due to the increase in the penetration of the highspeed broadband and of the wireless networks; to the centralization of computer resources and the broad adoption of cloud computing; to the proliferation of IP and connected devices; and to the growing of user interfaces, with the appearance of new technologies which are potentially disruptive. On the other hand, the data explosion will occur due to the increase in the sharing of confidential information among the organizations and the individuals; to the bigger number of persons globally connected; to the multiplication of devices and applications generating traffic; and to the higher need for classification of information.

With the massive distribution of information, either through the corporate networks or through the Internet, being accessed by the most varied devices, the concern with its security has increased among its holders, leading to a continuous search for really efficacious measures for its protection. The reason for this concern is reflected, according to Dantas (2011), in the fact that the information has become the most precious asset for the businesses of an organization, and its absence, or its leakage, may lead a company to extinction.

In spite of the efforts of the ICT managers regarding the implementation of control mechanisms, which aim at ensuring the protection of the information, it is necessary to take into account the understanding and the adoption of such technologies by its users. According to Dantas (2011), the involuntary leakage of information occurs during the performance of routine actions of the organization, which places the human resources as one of the biggest concerns at the implementation of policies and training programs geared towards the security of information.

CC BY

There is a perceived absence of studies on the understanding and adoption of technologies destined to the Information Security Management, geared towards the sphere of the Brazilian National Defense, in which sensitive information, with a strategic nature to the country, is made available through the use of tools with access available through the internal corporate network or even through the Internet.

The organization selected for the conduction of this study was the Brazilian Air Force Information Technology Board - DTI, having in view it is a central authority of the Information Technology System within the Air Force Command – COMAER and it has had is purpose defined as "standardizing, planning, implementing, coordinating controlling, and inspecting the activities related to Information Technology of the Air Force Command" (BRASIL, 2015, p. 7).

In order to include a more heterogenous group, the target audience of this research was chosen as the Government Agents belonging to DTI staff, which is a group consisting of "every individual who, vested with attributions and responsibilities defined in a specific act, performs administrative activities of budget, financial, accounting, property, and human resources management of COMAER" (BRASIL, 2014, p. 10). The sample consisted of officers and noncommissioned officers of DTI staff, belonging to the technical, administrative, and managing areas, which hereinafter, for the purposes of this study, will be referred to as DTI staff or simply staff.

Therefore, this scientific work has the general purpose of analyzing the factors which influence the DTI staff in relation to the understanding of the Information Security Management practices. This way, the following question has arisen: which factors influence the DTI staff in relation to the understanding of the Information Security Management practices?

In order to answer the question above, the following hypotheses were made, which could be demonstrated by the result of this research: H_1. The sociodemographic profile of the staff has a significant influence on the understanding of the Information Security practices; H_2. The perceptions of the staff in relation to the ease of use and usefulness of the security practices have a significant influence on the understanding of the Information Security practices; H_3. The behavioral profile (attitude) of the staff has a significant influence on the understanding of the Information Security practices; and H_4. The intention of use of the security practices has a significant influence on the understanding of the Information Security practices.

With the purpose of guiding the research actions, so as to achieve the general objective, the following specific objectives were established: O_1. To identify, in the DTI staff, their respective sociodemographic and behavioral profiles, as well as their perception of the ease of use and the usefulness of the Information Security practices; O_2. To assess the perception of understanding of the DTI staff in relation to the Information Security Management practices, in conformity with the NBR 27001 (2013) guidelines; and O_3. To verify the existing relations of sociodemographic profile, perceived ease of use, perceived usefulness, attitude, and behavior of the DTI staff, to the level of understanding of the Information Security Management standards.

The relevance of this research is demonstrated by the fact that DTI is the central authority of the Brazilian Air Force Information Technology within COMAER and by its influence on the other organizations which are part of this system, and it may modify the view of such authorities as to the importance of the perception of the users in relation to the understanding of the control mechanisms which aim at guaranteeing the information security.

CC BY

INFORMATION SECURITY MANAGEMENT AND TECHNOLOGY ACCEPTANCE MODEL

This topic is destined to a brief introduction of concepts related to the Information Security Management and to the security standards NBR 27001 (2013) and 27002. In addition to these, the concepts related to the Technology Acceptance Model and the relations established between the constructs, whose investigation is intended, will be introduced.

Information Security

For the proposed topic to be deeply studied, it is necessary to understand the meaning of the term Information Security. According to the manual of Information Security Good Practices published by TCU (BRASIL, 2012, p. 9), the information security aims at "safeguarding the integrity, the confidentiality, the authenticity, and the availability of the information processed by the institution".

The information security, according to NBR 27002 (2013), is achieved from the implementation of a set of proper controls, including policies, processes, procedures, organizational structures, and functions of software and hardware. Those controls need to be established, implemented, monitored, critically analyzed, and improved, in order to ensure that the objectives of the business and the information security of the organization are achieved.

According to Silva et al (2003), the information security is a complex process, with technological and human components, involving methodologies and behaviors. He goes on to affirm that, in order to allow the implementation of the desired models, we need to learn the human aspects of the organization, in which case it is necessary to outline the profile, as much as possible, of the direct and indirect participants in the organization security.

Another important term for the understanding of this study is the concept of vulnerability. Every vulnerability is closely related to the weakest point of an asset and must be dealt with as a frailty. The vulnerabilities may arise as a result of a processing error (failure in the systems code), of a failure of an agent, or of the bad configuration of applications, either intentional or not, causing the generation of unreliable information, which implies the violation of one or more principles of information security (LYRA, 2015).

According to Lyra (2015, apud LYRA, 2008), such vulnerabilities may be explored or not, and it is possible for an information asset to present a weakness which will never be effectively affected by it. Dantas (2011) and Sêmola (204) classify the vulnerabilities according to the following origins: natural, organizational, physical, hardware, software, storage means or media, human, and communications.

In order to achieve the objectives of this study, only the human vulnerabilities were considered, having in view that, in spite of all controls proposed by the information security standards, the human factor is still considered one of the biggest problems to the Information Security Management.

According to Sêmola (2014), the human resources are considered the most fragile point of the information security process, being responsible for one or more of its stages. Sêmola (2014) adds that, even if standards are specified for the creation, handling, storage, transport, and discard of passwords, and if technological resources of audit and access authentication are implemented, so as to provide a safer environment, we may still have the efficiency of such practices doubted if a worker does not comply with the instructions of the security policy, sharing his or her access credentials, which are supposedly personal and untransferable.

CC BY

Corroborating the teachings of Sêmola (2014), Dantas (2011) considers that the human vulnerabilities represent the biggest concern to the specialists, having in view that the noncompliance with or disregard of security measures is the biggest vulnerability to the information security process. Dantas (2011) also affirms that the origin of such vulnerabilities may be related to the lack of specific qualification for the development of activities which are inherent in the function of each individual, to the lack of security awareness in face of routine activities, mistakes, omissions, discontent, recklessness in the creation and confidentiality of passwords and of the failure to use cryptography in the communication of confidential information.

Sêmola (2014) also emphasizes that the risks related to the vulnerabilities inherent in the human resources need to be dealt with so as to consolidate an organizational culture of security. For that, the author recommends a strategy of sharing of the information security responsibility with each individual of the institution, which requires the broad understanding of the information security practices in force by the workers. After all, according to the same author, the level of security of a chain is equivalent to the resistance of its weakest link.

NBR 27001 (2013), which governs the information security management system, defines the following areas as objectives of control: Information security policies (A.5); Information security organization (A.6); Security in human resources (A.7); Asset management (A.8); Access control (A.9); Cryptography (A.10); Physical security and security of the environment (A.11); Security in operations (A.12); Security in communications (A.13); Acquisition, development, and maintenance of systems (A.14); and Relations in the chain of supply (A.15). NBR 27002 (2013), on its turn, governs the code of practice for the information security controls, defines the implementation guidelines for each one of the objectives of control established by NBR 27001 (2013).

For the purpose of this research, the practices related to the domains Security in human resources (A.7) and Access controls (A.9) were chosen, having in view the relevance of these domains from the perspective of the users.

Technology Acceptance Model

Another theoretical base supporting this study is related to the acceptance and adoption of technologies destined to the information security. One of the most known and broadly used theoretical models to assess the perception of the users in relation to their acceptance of a certain technology is the TAM mode. This model and its adaptations were broadly tested by several organizations and several studies, as observed in Gabbay (2003); Netto e Silveira (2007); Nobre (2009); Silva et al (2009); Silva et al (2008); and Vilar (2013).

According to Silva et al (2008, apud STÉBILE, 2001), such studies appeared by virtue of the development of new technologies, geared towards the processing and dissemination of information and of the influence of these technologies on the behavior of the contemporary society. Mostly, the information systems were created having as their focus the technologies employed and not their strategic use or its adjustment to the users.

According to Nobre et al (2010, apud DAVIS; BAGOZZI; WARSHAW, 1989), the TAM model is supported by two constructs based on belief, which are the perceived ease of use and the perceived usefulness. According to Nobre et al (2010), the perceived ease of use is related to the expectation of the user not to make any physical or mental effort when using technology, while the perceived usefulness is related to the perception by the user of an improvement in the development or his or her activities with the use of technology.

CC BY

Still according to the writings of Nobre et al (2010), the TAM model predicts the relation between the perceived ease of use and the perceived usefulness with two other constructs, the attitude, which is defined as an individual feeling (positive or negative) in relation to a behavior one may have, and the behavioral intention, which is understood as the level with which a person has the intention of developing a certain behavior.

Therefore, the TAM model proved appropriate, by means of a simple adaptation, to the conduction of the test in the hypotheses proposed in this study, so as to prove them, and thus leading to the answer to the initial question of this research.

METHODOLOGY

In order to achieve the objective proposed for this work, it was based in the hypothetical-deductive method, which, according to Prodanov (2013), begins with the preparation of a research problem or the identification of a loophole in the scientific knowledge, followed by the formulation of hypotheses and by a process of deductive inference, which is responsible for validating or refuting the prediction of the occurrence of phenomena contained in such hypotheses.

In relation to its objective, this research had a descriptive nature, for, according to Gil (2008, p. 28), it has "as a main objective the description of the characteristics of a certain population or phenomenon or the establishment of relations among variables", as to the approach of the problem, it was classified as quantitative, which means, according to Prodanov (2013), that it aims at translating opinions and information into numbers in order to classify them and analyze them, using resources and statistical techniques.

From a technical point of view, the data for the conduction of this research were gathered by means of survey, having in view that, according to Prodanov (2013), this type of research occurs when it involves direct questions to the individuals, whose behavior we wish to learn, by means of the application of some type of questionnaire, in which case the information regarding the studied problem is requested from an expressive group of people, so that, right after that, the conclusions may be reached from the data collected, by means of a quantitative analysis.

In this regard, the collection of the data studied by this research was by means of the application of a questionnaire to 58 military servants and civilians belonging to the DTI staff. The questionnaire was based on the precepts from NBR 27001 (2013) and from NBR 27002 (2013), which govern, respectively, the Information Security Management System and the code of practice for the information security controls. The selection of the method of collection was due to its advantages in relation to the interview, of which we can highlight, according to Gil (2008), the guarantee of the anonymity of the answers, the fact that it allows people to answer it whenever they deem convenient, and the non-exposition of the subjects to the influence of the opinions and of the personal aspect of the interviewer.

The questionnaire adopted to this study consists of multiple choice questions, with three parts (Appendix 1). The first part is destined to identifying the sociodemographic information related to the staff researched, such as age, sex, education, general knowledge of computers, level of qualification in Computer Networks and Information Security, role performed in the adoption of new technologies in the organization, use of the network of the organization to access personal accounts and practice in the creation of backup.

In the second part of the questionnaire has the dependent variables, adapted to the TAM model. This part of the questionnaire had the objective of collecting answers in relation to beliefs

CC BY

and perceptions related to the constructs ease of use, perceived usefulness, attitude, and behavioral intentional in the face of the information security practices. For these items, Likert scales were used in five levels of measurement, from "totally disagree" to "fully agree". This part of the questionnaire also included the questions on the behavioral intention to use the information security practices. These questions consisted of a scale with five levels of agreement, ranging from "highly unlikely" to "highly likely".

Finally, the third part of the questionnaire included the questions aiming at identifying the level of understanding of the staff in relation to the information security practices in force, included in NBR 27001 (2013) and in the DTI information security policy, with emphasis on the access controls and human resources controls. These questions had five levels of measurement, ranging from "totally disagree" to "fully agree".

For the purposes of this research, a subtle adaptation of the TAM model was also performed, so that it enabled the identification of the level of understanding of the information security practices by the users, as opposed to the original model, which aims at identifying the acceptance, and for that only the verbal replacement of the statements inserted in the third part of the applied questionnaire was necessary.

Subsequently, after the collection of the data, they were tabulated and analyzed, in order to test the relations existing between the sociodemographic profile, the perceived ease of use, the perceived usefulness, the attitude, and the behavior of the Brazilian Air Force Information Technology Board - DTI staff, and the level of understanding of the Information Security Management standards, by means of procedures of descriptive statistics and of the application of Fisher's exact test, having in view that the number of answer of several variables was lower than five (LARSON; FARBER, 2010).

According to Marconi and Lakatos (2003), the role of the statistical method is to be responsible for providing a quantitative description of society. Still according to the author, the statistics may be considered more than just a means of rational description, being also a method of experimentation and proof, for it is a method of analysis.

The statistical procedures allow us to achieve, from complex groups, simple representations, and to check whether these simplified verifications are related among themselves. According to the authors, the statistical method means the reduction of sociological, political, and economic phenomena, among others, to quantitative terms and to a statistical manipulation, which allows us to prove the relations of the phenomena among themselves and to achieve generalizations about their nature, occurrence, or meaning.

The descriptive statistics is the method by means of which the numeric data are collected, organized, and classified, so as to enable their presentation and the definition of characteristics which allow their analysis and interpretation, and it may be performed in quantitative or qualitative variables (SINDELAR et al, 2014).

The dependency among the variables was conducted by means of the comparison between two hypotheses, respectively called null hypothesis and alternative hypothesis. The null hypothesis is that the variables are not associated; in other words, they are independent. The alternative hypothesis is that the variables are associated, that is, they are dependent (LARSON; FARBER, 2010).

The associations in which the p-value achieved, by means of the application of the Fisher's test, was lower than or equal to 0.05, with a reliability percentage of 95%, or lower than 0.001, with reliability of 99%, were considered.

CC BY

Based on the methodology employed, it was possible to analyze the hypotheses raised in the beginning of the article, which consider that: H_1: the sociodemographic profile of the staff has a significant influence on the understanding of the Information Security practices; H_2: the perceptions of the staff in relation to the ease of use and usefulness of the security practices have a significant influence on the understanding of the Information Security practices; H_3: the behavioral profile (attitude) of the staff has a significant influence on the understanding of the Information Security practices; H_4: and the intention of use of the security practices has a significant influence on the understanding of the Information Security practices.

PRESENTATION AND DISCUSSION OF THE RESULTS

After the collection and tabulation of the data, it was possible to identify the sociodemographic profile of the DTI staff by means of the answers collected by the first part of the questionnaire applied, allowing a better knowledge about the human aspects of the organization, as highlighted by Silva et al (2003), as it can be observed in Table 1.

As to the gender, it was verified that most individuals surveyed are male (70.7%). In relation to age, the DTI staff proved to be highly heterogeneous, with the biggest concentrations in the groups between 26 and 35 years of age (39.7%) and between 46 and 55 years of age (29.3%). Another information raised was the area of the participants, in which case nearly half the staff belong to the administrative area (48.3%), and the other individuals are distributed among the areas of IT management or governance and the technical area, which was already expected, once DTI is an organization destined to the management and control of the Brazilian Air Force IT System.

The level of education of the staff was another characteristic researched, and it was possible to verify that most of the DTI staff has completed higher education (36.2%) and an expressive number of individuals has some kind of specialization or MBA (25.9%).

In relation to the knowledge of computers, it was noticed that nobody declared to be lay and the great majority (44.8%) has advanced knowledge of the topic. As to the qualification in networks or information security, the biggest part of the staff (39.7%) declared not to have any knowledge of the subject.

The individuals were also questioned as to the participation in the adoption of new technologies, and it was observed that the great majority of the staff (72.44%) participate only as users.

Finally, the participants in the research were questioned as to the use of the organization network to access personal accounts and to the frequency of creation of backup, and it was found out that a very expressive group of users (58.6%) affirmed to sometimes use the network for that purpose, and another smaller group (17.2%) admitted to always using the corporate network to access personal accounts. Regarding the frequency of creation of backup, it was possible to observe that most users (39.7%) create backup only sometimes, but another very representative group (27.6%) is used to always making a backup copy it their information.

Subsequently, Table 2 presents the indices of agreement of the DTI staff about six statements structured according to the TAM model. The consolidated data show a great dispersion as to the agreement of the individuals with the mental effort necessary to use IS practices. Still in relation to the ease of use, 67.2% of the individuals affirm to agree, in full or in part, that they find it very easy to use the IS practices. As to the perceived usefulness, there is a great

CC BY

Table 1. Sociodemographic Data

Statements	Categories	Indexes
Area of the participants	Administrative area	48,3%
	IT management or governance	29,3%
	Technical area	22,4%
Age	Less than 25 years	1,7%
	From 26 to 35 years	39,7%
	From 36 to 45 years	19,0%
	From 46 to 55 years	29,3%
	Over 55 years	10,3%
Gender	Male	70,7%
	Female	29,3%
Level of education	Medium	10,3%
	Higher Education	17,2%
	Higher Complete	36,2%
	Specialization or MBA	25,9%
	Masters or Doctorate	10,3%
	Other	0,0%
Knowledge of computers	No knowledge	0,0%
	Basic Knowledge	19,0%
	Knowledge intermediaries	36,2%
	Advanced Knowledge	44,8%
Qualification in networks or information security	No knowledge	39,7%
	Basic Knowledge	20,7%
	Knowledge intermediaries	19,0%
	Advanced Knowledge	20,7%
I participate in the adoption of new technologies in my organization	Only as a user	72,4%
	In the definition of specifications	20,7%
	In the authorization of adoption	6,9%
I use organization network to access personal accounts	Always	17,2%
	Almost Always	3,4%
	Sometimes	58,6%
	Almost Never	12,1%
	Never	8,6%
Frequency of creation of backup	Always	27,6%
	Almost Always	15,5%
	Sometimes	39,7%
	Almost Never	10,3%
	Never	6,9%

Source: Data from the survey.

concentration of individuals who agree, in full or in part, that such practices make their work more efficient and are extremely important to its performance. In relation to the attitude, once again there is a great dispersion in the answers as to the agreement of the individuals with liking and adopting IS practices.

CC BY

Table 2. Information Security practices

Statements	TAM construct	1	2	3	4	5
Use of Information Security practices requires a lot of my mental effort.	Perceived ease of use	22,4%	37,9%	15,5%	20,7%	3,4%
I have a lot of ease in the use of Information Security practices.	Perceived ease of use	0,0%	8,6%	24,1%	44,8%	22,4%
Adoption of Information Security practices makes my work more efficient.	Perceived usefulness	0,0%	8,6%	24,1%	43,1%	24,1%
Use of Information Security practices is extremely important to performance of my work.	Perceived usefulness	0,0%	13,8%	12,1%	37,9%	36,2%
I like to use Information Security practices.	Attitude	1,7%	5,2%	17,2%	51,7%	24,1%
Using Information Security practices makes my work more interesting.	Attitude	5,2%	15,5%	24,1%	37,9%	17,2%

1 - I totally disagree; 2 - I disagree; 3 - I do not agree nor disagree; 4 - I agree; and 5 - I completely agree.
Source: Data from the survey.

Table 3 shows the percentages related to the behavioral intention of the individuals as to the use of the IS practices. In relation to this aspect, there is a great concentration of answers, in both statements, showing that the use of the IS practices by the DTI staff is likely or highly likely.

Finally, Table 4 shows the descriptive results of the understanding of the individuals as to the application of the IS practices included in NBR 27001 (2013). In this part of the questionnaire, the questions with the highest level of agreement by the researched individuals are related to the control of single access per user (4.7), to the commitment to secrecy in writing (4.3), and to the monitoring and recording of the facilities (4.3); while the questions with the lowest levels were about the physical access by biometry (3.0), and the investigation of the background of new users (3.0).

For the conduction of the analysis of the data of this research, in relation to the understanding of the application of the IS practices, the means equal or above 3.5 were considered positive, and the lower means were considered negative.

After the process of descriptive analysis of the data, the statistical treatment was performed with the sociodemographic data and the level of understanding of the IS practices, by means of the application of Fisher's exact test, with the achievement of the p-value indices presented in Table 5.

By observing the results achieved, we can perceive that few sociodemographic factors have a significant association with any of the understandings of IS practices investigated. Among the sociodemographic factors, the Performance Area of the Respondent was the factor with the biggest number of associations, thus significantly influencing (p-value <= 0.05) the understanding of the practices of: regular review of access rights; prohibition of reusing passwords; existence of monitoring or recording of the facilities; clear rules of liability for misuse; and disciplinary proceedings for users who made mistakes.

The understanding of the practices of regular review of access rights was clearly and negatively influenced (mean 3.2) by the answers of the individuals of the administrative area, where the majority (46.43%) informed not to agree or to disagree with the adoption of such practice. In relation to the practice of prohibition of reusing passwords, there was the same trend of negative influence (mean 3.4), in which the great majority of the individuals of the administrative area (60.71%) informed not to agree or to disagree with the implementation of this practice, contrasting with the representatives of the technical area, in which only a small portion (23.08%) chose this answer.

CC BY

Table 3. Behavioral intention as to use of the Information Security.

Indicators	TAM Constructs	1	2	3	4	5
If I have access to the standards of practice for information security, i want to use them.	Behavioral intention	0,0%	1,7%	10,3%	46,6%	41,4%
Since I have access to the standards of Information Security, I predict that the us.	Behavioral intention	0,0%	5,2%	10,3%	50,0%	34,5%

1 - Highly unlikely; 2 - Unlikely; 3 - I do not know; 4 - Probable; and 5 - Highly probable.
Source: Data from the survey.

The scenario presented above demonstrates the lack of knowledge of the security rules, mainly by the individuals of the administrative area, which was mentioned by Dantas (2011) as the biggest vulnerability of the IS process of an organization and by Sêmola (2014) as responsible for casting doubt on the efficiency of such practices.

On the other hand, the practice related to the existence of monitoring or recording of the facilities was positively influenced (mean 4.3) by the individuals of the technical area, where the great majority (76.92%) fully agree with such practice being implemented at DTI, and by the individuals of the administrative area, of which a great part (53.57%) also agreed with such answer. Another practice which was positively influenced (mean 3.7) regards the existence of clear rules of liability for misuse of IT resources, and this influence was made possible thanks to the quantity of individuals from the technical area who agreed (38.46%) or fully agreed (46.15%) with the perception of application of this practice, even with a large number of individuals of the administrative area (46.43%) who informed not to agree or to disagree with such practice.

However, the practice which establishes disciplinary proceedings for users who make mistakes was negatively influenced (mean 3.3), both by the number of individuals from the administrative area (67.86%) and by the ones from the management or governance area (58.82%), who reported not to agree or to disagree with the implementation of this practice at DTI, once again highlighting the lack of knowledge of the security practiced as mentioned by Dantas (2011).

Other sociodemographic factors which demonstrated the significant association (p-value <= 0.05) with the understanding of the staff were the Participation in the Adoption of New Technologies, influencing the practice of disciplinary proceedings for users who made mistakes, and the Use of the Computer Network to Access Personal Accounts, which influenced the understanding of the existence of monitoring or recording of the facilities.

The factor of Participation in the Adoption of New Technologies also corroborated the negative influence (mean 3.3) on the perception of the practice of disciplinary proceedings for users who made mistakes, such influence being clearly related to the individuals who participated only as users in the process of adoption of new technologies, that is, the biggest part of the DTI staff, in which the great majority (64.29%) alleged not to agree or to disagree with such practice being effectively applied, showing the absence of an organizational culture of security on the issue, as emphasized by Sêmola (2014).

On its turn, the sociodemographic factor related to the Use of the Computer Network to Access Personal Accounts proved to be positively related (mean 4.3) to the existence of monitoring or recording of the facilities, having in view that the great majority of the users (80%) who never used the corporate network of the organization to access personal accounts fully agree with the security practice being applied to the DTI and an expressive amount of individuals (71.43%), who rarely follow such practice, also have the same understanding of the issue.

CC BY

Table 4. Level of understanding as to the application of the Information Security practices

Statements	Dimension	Mean	1	2	3	4	5
Access token only per user.	CA	4,7	0	0	4	9	45
Compromise of confidentiality of users by writing.	CA	4,3	1	2	12	8	35
Reactivation of password via identification details.	CA	3,7	1	11	13	11	22
Regular review of access rights.	CA	3,2	5	7	23	15	8
Warning to avoid password recorded on paper.	CA	3,9	1	7	15	11	24
Mandatory password change regularly.	CA	3,2	9	8	15	15	11
Limitation of five attempts to login.	CA	3,1	4	6	36	5	7
Prohibition on reuse of passwords.	CA	3,4	3	7	27	6	15
Special precautions for use of resources of mobile computing.	CA	3,4	3	4	26	14	11
Removal of access for users off.	CA	3,6	1	8	19	15	15
Physical access to biometrics.	CA	3,0	14	5	16	12	11
Existence of monitoring or recording of installations.	CA	4,3	0	0	16	10	32
Clear rules of accountability for misuse.	RH	3,7	1	5	19	16	17
Research of the past of the user.	RH	3,0	5	7	35	5	6
Document Signing of responsibility for new users.	RH	4,1	1	4	15	9	29
Receiving adequate training.	RH	3,1	8	11	18	11	10
Disciplinary procedures for users who make mistakes.	RH	3,3	2	4	33	11	8
Formal procedure for creating new user.	CA	3,9	2	6	12	13	25

CA - Access Control dimension; and RH - Human Resources dimension.
1 - I totally disagree; 2 - I disagree; 3 - I do not agree nor disagree; 4 - I agree; and 5 - I completely agree. Source: Data from the survey.

After that, the statistical treatment was performed with the collected data by the answers related to the constructs of the TAM model and the level of understanding of the IS practices, with the application of the same tests previously used, and the results (p-value) are in Table 6.

With the statistical results it was possible to observe that the construct perceived ease of use of the TAM model has a significant positive influence (p-value <= 0.001) on two information security practices: use of single access identifier per user (mean 4.7) and clear rules of liability for misuse (mean 3.7).

The influence of the construct perceived ease of use on the understanding of the practice of single access per user was due to the fact that all individuals (100%) who fully agreed and to the great majority (84.62%) of the ones who agreed with the fact that there is a lot of ease in the use of IS practices also agreed with the application of this practice.

In the same way, the perceived ease of use influenced the understanding of the practice of clear rules of liability for the misuse of the network resources, due to the fact that a great part of the individuals (69.23%) who fully agree with the fact that they find it very easy to use the IS practices also agree with the application of this practice and that half (50%) of the individuals who have the same ease also agree with such practice.

Another TAM construct which significantly influenced (p-value <= 0.05 and p-value <= 0.001) in a positive way the perception of the researched individuals was the perceived usefulness, exercising such influence on the practices of: warning to avoid a password written on paper (mean 3.9), clear rules of liability for misuse of network resources (mean 3.7) and reactivation of password by means of a rigorous identification of the user (mean 3.7).

CC BY

Table 5 – Statistical treatment with the sociodemographic data

	Performance Area of the Respondent	Age	Gender	Level of Education	Knowledge of computers	Qualifications in networks or information security	Participation in the adoption of new technologies	Use organization network to access personal accounts	Frequency of creation of backup
Single access identifier per user	0,2744	0,3002	0,4567	0,8627	0,0589	0,6354	0,9045	0,8806	0,4228
Commitment of confidentiality of users in writing	0,3145	0,8024	0,5018	0,6934	0,8554	0,8817	0,3365	0,5073	0,9264
Password re-activation via strict identification	0,1405	0,1968	0,6630	0,9472	0,8056	0,3565	0,3574	0,8288	0,2560
Regular review of access rights	**0,03096** (*)	0,5008	0,5423	0,9640	0,5240	0,9709	0,1926	0,5504	-
Alert to prevent password recorded on paper	0,1647	0,5818	0,8816	0,2830	0,8316	0,7332	0,3889	0,7853	0,6589
Obligation to change password regularly	0,6589	0,6416	0,4828	0,5616	0,0576	0,6487	0,5265	0,6904	0,9857
Limitation of five login attempts	0,7439	0,3455	0,6297	0,6972	0,7839	0,7614	0,2910	0,6945	0,2471
Prohibition of reusing passwords	**0,03815 (*)**	0,7122	0,7882	0,9134	0,1284	0,2297	0,5453	0,3939	0,9521
Special care for use of mobile computing resources	0,4998	0,6059	0,4364	0,2854	0,7144	0,3270	0,0674	0,3083	-
Removing access for disconnected users	0,6866	0,4802	0,3474	0,3259	0,7140	0,5273	0,1646	0,0755	-
Physical access by biometrics	0,1624	0,0629	0,0734	0,4892	0,6627	0,4484	0,3077	-	-
Existence of monitoring or recording of the facilities	**0,0453 (*)**	0,3187	0,4200	0,9105	0,5018	0,5129	0,7463	**0,02303 (*)**	0,4536
Clear rules of liability for misuse	**0,01257 (*)**	0,7609	0,8897	0,3589	0,2129	0,7518	0,4960	0,6535	-
Investigation of the user's past	0,1471	0,8395	0,6859	0,1275	0,9233	0,1650	0,7626	0,5097	-
Signing of responsibility document for new users	0,2514	0,1222	0,8818	0,7640	0,4610	0,2399	0,2512	0,3293	0,1157
Receipt of adequate training	0,5380	0,5423	0,5244	0,9419	0,5576	0,8768	0,2963	-	-
Disciplinary proceedings for users who made mistakes	**0,04798 (*)**	0,8681	0,9819	0,8443	0,2711	0,3116	**0,01733 (*)**	0,7644	0,5795
Formal procedure for creating new user	0.1011	0.5508	0.7731	0.8175	0.3481	0.2818	0.2778	0.8553	0.6199

(*) p-value <= 0,05
(**) p-value <= 0,001 Source: Data from the survey.

CC BY

Table 6 – Statistical treatment of TAM model constructs and the level of understanding of the IS practices

	Perceived ease of use		Perceived usefulness		Attitude		Behavioral intention	
	Use of Informations Security practices requires a lot of my mental effort	**I have a lot of ease in the use of Information Security practices**	**Adoption of Information Security practices makes my work more efficient**	**Use of Information Security practices is extremely importante to performance of my work**	**I like to use Information Security practices.**	**Using Information Security practices makes my work more interesting.**	**If I have access to standards of Information Security practices, I intend to use them**	**Given that I have access to standards of Information Security practices, I foresee that I would use them.**
Use of single access identifier per user	0,1020	**0,0098 (**)**	0,7757	0,2243	0,3596	0,8341	**0,0276 (*)**	**0,0101 (*)**
Commitment of confidentiality users in writing	0,6607	0,0927	0,6432	0,1807	0,0663	0,6940	0,1956	0,0631
Reactivation of password by means of a rigorous identification of the user	0,9120	0,4489	0,3755	**0,0223 (*)**	0,6630	0,4603	0,6731	**0,0339 (*)**
Regular review of access rights	0,2336	0,6177	0,7773	0,4319	0,1832	0,8560	0,1627	0,6711
Warning to avoid a password written on paper	0,9595	0,4642	**0,0383 (*)**	0,1099	0,0890	0,2185	**0,0478 (*)**	0,4462
Obligation to change password regularly	0,7698	0,1779	0,7390	0,8661	0,2579	0,8627	0,6792	0,6885
Limitation of five login attempts	0,7539	0,6026	0,3771	0,5598	0,5006	0,0985	0,9353	0,2555
Prohibition of password reuse	0,7444	0,4208	0,5838	0,3735	0,4554	0,1150	0,9551	0,9626
Special care in relation to the use of mobile computing resources	0,7046	0,5172	0,5374	0,5824	**0,0027 (*)**	erro	0,3637	**0,0018 (*)**
Removing access for disconnected users	0,5055	0,7586	0,7882	0,9985	0,1932	erro	0,5119	0,1527
Physical access by biometrics	erro	0,7240	0,2754	erro	0,3528	erro	0,4950	0,3117
Existence of monitoring or recording of installations	0,8261	0,3553	0,4704	0,4605	0,5640	0,6987	0,5489	0,1270
Clear rules of liability for misuse	0,1283	**0,0002 (**)**	**0,0007 (**)**	0,2467	0,4689	erro	0,1564	0,1869
Investigation of the user's past	0,8886	0,4205	0,2021	0,6250	0,0567	0,6570	0,8321	0,4484
Signing of responsibility document for new users	0,6655	0,8567	0,3678	0,0931	0,2338	0,4649	0,0020	0,3601
Receipt of adequate training	0,5754	0,8698	0,2985	0,6948	0,6264	0,6517	0,6372	0,1863
Disciplinary Procedures for Users Who Make Errors	0,9424	0,9303	0,5870	0,8815	0,9311	0,7824	0,5637	0,2903
Formal procedure for creating new user	erro	0,1053	0,6570	0,1342	0,6275	0,7950	0,3135	0,3629

(*) p-valor <= 0,05; *(**) p-value <= 0,001*
Source: Data from the survey.

CC BY

In relation to the influence of the perceived usefulness on the understanding of the practice of warning to avoid the writing of passwords on paper, it was noticed that the it occurred due to the fact that most part (57.14%) of the individuals who fully agree that the adoption of IS practices makes the work more efficient also fully agree with the application of such practice at DTI.

In relation to the influence of such TAM construct on the understanding of the practice of existence of clear rules of liability for misuse of the network resources, it was noticed that such influence was due to the fact that half (50%) of the individuals who fully agree that the adoption of IS practices makes the work more efficient also fully agree with the application of such security practice and that a great part (48%) of the ones who agree that IS practices make the work more efficient also agree that this practice is implemented.

Still about the influence of the perceived usefulness, but about the understanding of the practice of reactivation of password by means of a rigorous identification of the user, it could be perceived that it was based on the fact that a great part of the individuals who fully agree (42.86%) and who agree (40.91) that the use of IS practices is extremely important for the performance of the work also fully agree with the fact that such practice has been applied.

The attitude was the construct demonstrating less significant influence (p-value <= 0.05) on the perception of the individuals of the implementation of IS practices and the influence was negative (mean 3.4) on the practice of special care in relation to the use of mobile computing resources.

The influence of the construct attitude, about the perception of the practice of special care in relation to the use of mobile computing resources, was due to the fact that the biggest part of the individuals who fully agree (57.14%) or agree (36.67%) with the fact that they like using the Information Security practices do not agree or disagree with the application of the security practiced mentioned, which once again calls the attention to the lack of knowledge of the individuals as mentioned by Dantas (2011).

Finally, the TAM construct with the biggest number of significant influences (p-value <= 0.05) on the perception of IS practices was the behavioral intention, having a positive effect on the practices: existence of a single access identifier per user (4.7), reactivation of password by means of a rigorous identification of the user (mean 3.7), and warning to avoid the writing of passwords on paper (mean 3.9); and a negative effect on the practice: special care for the use of mobile computing resources (mean 3.4).

The influence of the behavioral intention on the perception of the practice which provides for the existence of a single access identifier per user was emphasized with the answer to two questions: it I have access to the IS, I intend to use them, in which nearly all users (91.67%) who consider its use highly likely also fully agreed with the application of such practice; and having access to the IS rules, I would expect to use it, in which the majority (95%) of the individuals who affirmed to expect to use the rules also fully agreed with the existence of this practice.

Another practice which was influenced by the behavioral intention was the reactivation of password by means of the rigorous identification of the user, induced by the great number of individuals (48.28%) who consider the use of IS rules likely, who also fully agree with the application of the practice mentioned.

The influence of the behavioral intention on the perception of the practice which prescribes the existence of warning to avoid the writing of passwords on paper was highlighted by the fact that half (50%) of the individuals who consider it highly likely and a great number (40.74%) of those who consider likely the fact that they intend to use the IS rules if they have access to them also fully agree with the fact that such practice is applied at DTI.

CC BY

On the other hand, the behavioral intention was demonstrated to negatively influence the perception of the individuals about the practice of special care for the use of mobile computing resources, which was observed due to the fact that most individuals (60%) who affirmed to expect to use the IS practices, for having access to the rules, do not agree or disagree with the application of such practice, which once again demonstrates the lack of awareness of security, in view of routine activities (DANTAS, 2011).

FINAL COMMENTS

Based on the achievement of the specific objectives establish to guide this study, by means of the collection and analysis of the data, by means of the application of proper statistical methods, it was possible to demonstrate the hypotheses raised by the researchers.

Hypothesis H_1, according to which the sociodemographic profile of the staff has a significant influence on the understanding of Information Security practices, may be demonstrated by the significant influence of the sociodemographic factors: performance area of the respondent, participation in the adoption of new technologies, and use of the computer network to access personal accounts. The demonstration of hypothesis H_1 leads to the observation that only the individuals with a direct contact with the IS rules and practices understand their need and importance to the security of the information.

On its turn, hypothesis H_2, which assumes that the perceptions of the staff in relation to the ease of use and the usefulness of the security practices have a significant influence on the understanding of Information Security practices, was demonstrated by the significant influence of the indicators: to have ease in the use of IS practices, the perception that IS practices make the work more efficient, and the perception that the use of IS practices is extremely important to the performance of the work. The results of hypothesis H_2 leads to the reflection that the IS practices must take into account principles of usability and practicality in the application of the routine of an organization, otherwise they may no longer be practiced to the detriment to the execution of the main activities of the individual.

The affirmation of hypothesis H_3, which presumes that the behavioral profile (attitude) of the staff exercises a significant influence on the understanding of IS practices, could be demonstrated only by means of the significant influence of the indicator related to the liking of the use of IS practices, that is, only those individuals who have a bigger interest in IS understand the applied practices. Such observation is related to the institutionalization and broad disclosure of the IS rules and practices in all sectors dealing with classified information (SÊMOLA, 2011).

Finally, it was possible to demonstrate hypothesis H_4, which prescribed that the intention of using the IS practices exercises a significant influence on the understanding of Information Security practices, by means of the significant influence of its two indicators: if there is access to the IS rules, I intend to use them and, having access to the IS rules, I expect to use them. The analysis relates to factors as disclosure and awareness of the individuals about the IS practices applied within the organization, and emphasizes NBR 27001 (2013) in the item "Training, awareness, and competence" and NBR 27002 (2013) in the item "Awareness, education, and training in information security".

This way, the answer to the initial question of this research was possible, and it is possible to affirm that all factors researched – sociodemographic profile, perceived ease of use, perceived usefulness, attitude, and intention of use – influence the DTI staff, in a positive or negative manner, in relation to the understanding of the Information Security Management practices.

CC BY

As expected, once the DTI is an organization destined to the IT governance at COMAER and once great part of its staff consists of individuals with some technical training in IT, the great majority of the influences on the understanding by the staff of the application of IS practices had a positive nature (mean >= 3.5), as observed in a similar research, conducted by Nobre et al (2010).

Therefore, as said by Sêmola (2014), having in view that the level of security of a chain is equivalent to the resistance of its weakest link, we must highlight the importance off the consolidation of a bigger organizational culture of Information Security within the DTI, by means of the implementation of processes of awareness and qualification of its staff regarding the issue, especially in the groups which showed a higher level of ignorance of the IS practices applied, such as the individuals who are part of the administrative and management areas, and the group of individuals who participate only as user in face of the adoption of new technologies.

It must also be highlighted that this study does not extinguish all possibilities of research regarding the issue, having in view that it was based only in the IS practices related to the domains Security in human resources (A.7) and Access control (A.9) included in NBR 27001 (2013), and the application of such methodology on the other domains of such standard in future researches is possible and encouraged.

ACKNOWLEDGEMENTS

We thank the Exmo. Sr. Brig Eng RONALDO YUAN, Director of the Brazilian Air Force Information Technology Board.

REFERENCE

ABNT NBR ISO/IEC 27001. (2006). *Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos*. *Associação Brasileira de Normas Técnicas*.

ABNT NBR ISO/IEC 27002. (2013). *Tencologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação*. Brasil.

BRASIL. (2015). *Comando da Aeronáutica. Comando-Geral de Apoio. Regimento Interno da Diretoria de Tecnologia da Informação da Aeronáutica*. RICA 21-236. Rio de Janeiro, RJ.

BRASIL. (2014). *Comando da Aeronáutica. Regulamento de Administração da Aeronáutica*. RCA 12-1. Brasília, DF.

BRASIL. (2010). *Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações*. Livro verde: segurança cibernética no Brasil. Brasília: GSIPR/SE/DSIC.

BRASIL. (2012). T*ribunal de Contas da União. Boas práticas em segurança da informação*. 4. ed. Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação.

DANTAS, M. L. (2011). *Segurança da informação: uma abordagem focada em gestão de riscos* (1st ed.). Olinda: Livro Rápido.

CC BY

GABBAY, M. S. (2003). *Fatores influenciadores da implementação de ações de gestão de segurança da informação: um estudo com executivos e gerentes de tecnologia da informação das empresas do Rio Grande do Norte*. Dissertação (Mestrado). Universidade Federal do Rio Grande do Norte.

GIL, A. C. (2008). *Métodos e técnicas de Pesquisa Social* (6th ed.). São Paulo: Atlas S.A.

LARSON, R., & FARBER, B. (2010). *Estatística aplicada* (4th ed.). São Paulo: Pearson Prentice Hall.

LYRA, M. R. (2015). *Governança da Segurança da Informação*. Brasília: n.d.

MARCONI, M. de A., & LAKATOS, E. M. (2003). *Fundamentos de Metodologia Científica*. São Paulo: Atlas S.A.

NETTO, A. S., & SILVEIRA, M. A. P. (2007). Gestão da Segurança da Informação: fatores que influenciam sua adoção em pequenas e médias empresas. *Revista de Gestão Da Tecnologia E Sistemas de Informação*, *4*(3), 375–397.

NOBRE, A. C. S. (2009). *Fatores que influenciam a aceitação de práticas avançadas de Gestão de Segurança da Informação*. Dissertação (Mestrado). Universidade Federal do Rio Grande do Norte.

NOBRE, A. C. S., RAMOS, A. S. M., & NASCIMENTO, T. C. (2010). Fatores que influenciam a aceitação de práticas avançadas de Gestão de Segurança da Informação: um estudo com gestores públicos estaduais no Brasil. In *XXXIV Encontro da ANPAD*.

PRODANOV, C. C. (2013). *Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico* (2nd ed.). Novo Hamburgo: Feevale.

SÊMOLA, M. (2014). *Gestão da segurança da informação: uma visão executiva* (2nd ed.). Rio de Janeiro: Campus.

SILVA, P. M., DIAS, G. A., & ALMEIDA, J. R. (2009). Modelo de aceitação de tecnologia (TAM) aplicado ao Sistema de Informação da Biblioteca Virtual em Saúde (BVS) nas Escolas de Medicina da Região Metropolitana do Recife. *Informação & Sociedade*, *19*, 117–127.

SILVA, P. M., DIAS, G. A., & SENA JUNIOR, M. R. (2008). A importância da cultura na adoção tecnológica: o caso do Technology Acceptance Model (TAM). *Revista Eletrônica de Biblioteconomia E Ciência Da Informação*, *13*(26), 1–7.

SILVA, P. T., CARVALHO, H., & TORRES, C. B. (2003). *Segurança dos Sistemas de Informação: gestão estratégica da segurança empresarial*. Lisboa: Centro Atlântico.

SINDELAR, F. C. W., CONTO, S. M., & AHLERT, L. (2014). *Teoria e prática em estatística para cursos de graduação*. Lajeado: Univates.

VILAR, M. A. S. (2013). *Modelo de Aceitação da Tecnologia adaptado às compras online*. Universidade Fernando Pessoa.

CC BY

APPENDIX

PART I – THE RESPONDENT

(Please select only one of the alternatives in each question)

Respondent's field of work:

( ) Administration ( ) IT Management or Governance ( ) Technical

Age:

( ) Under 25 ( ) 36 to 45 ( ) Over 55

( ) 26 to 35 ( ) 46 to 55

Gender:

( ) Male ( ) Female

Education:

( ) High-School ( ) Higher Education with Specialization or MBA

( ) Incomplete Higher Education ( ) Higher Education with Master's Degree or Doctorate

( ) Complete Higher Education

( ) Other. Please specify: _____

General knowledge of informatics:

( ) No knowledge at all

( ) Basic knowledge (Windows, text editor, access to the Internet)

( ) Intermediate knowledge (basic + electronic worksheet and/or software for presentations)

( ) Advanced knowledge (intermediate + programming, database and/or webpage design)

Training in Computer Network and/or Information Security:

( ) No knowledge at all

( ) Basic knowledge (up to 40 hours of course)

( ) Intermediate knowledge (40 to 80 hours of course)

( ) Advanced knowledge (more than 80 hours of course)

I participate in the adoption of new technologies in my organization:

( ) Only as a user ( ) In the definition of specifications ( ) In the authorization for adoption

I use the organization's computer network to access personal accounts:

( ) Always ( ) Sometimes ( ) Never

( ) Often ( ) Hardly ever

I make backups of my files:

( ) Always ( ) Sometimes ( ) Never

( ) Often ( ) Hardly ever

CC BY

In order to answer the questions in parts II and III, the respondent shall understand that the **practices of Information Security (IS)** comprise an appropriate set of controls, including policies, processes, procedures, organizational structure and *software* and *hardware* functions. Some examples of Information Security practices are: the correct identification and verification of the reputation of those who will have access to the information; signature of the confidentiality or non-disclosure term; rating the information; notification of Information Security incidents; application of the clear desk and clear screen policies; use of credentials for access to information (passwords, tokens, etc.); formal authorization of requests to access information systems; periodical analysis of access rights; definition of rules for privileged access; use of single user ID; not reusing passwords; policy for passwords quality (complexity); not sharing passwords or tokens; making security copies (backup), among others.

PART II

(1) Totally disagree – the statement **does not correspond** to my perception on the theme.

(2) Disagree – the statement **does not correspond in total** to my perception on the theme.

(3) Neither agree nor disagree – **I do not have** an opinion on the theme.

(4) Agree – the statement **partially corresponds** to my perception on the theme.

(5) Totally agree – the statement **perfectly corresponds** to my perception on the theme.

Questions on user-friendliness, perceived usefulness and attitude

MARK AN "X" ACCORDING TO YOUR LEVEL OF AGREEMENT	1	2	3	4	5
1. The use of Information Security practices require great mental efforts on my side.					
2. It is very easy for me to use Information Security practices.					
3. The adoption of Information Security practices makes my work more efficient.					
4. The use of Security Information practices is extremely important for my work to be done.					
5. I enjoy using Information Security practices.					
6. Using Information Security practices makes my work more interesting.					

CC BY

(1) Highly improbable – **I do not have any** intention of using it.

(2) Improbable – **I do not have** intention of using it.

(3) I do not know – **I do not have** an opinion on my intention of using it.

(4) Probable – **I do have** some intention of using it.

(5) Highly probable – **I do have** great intention of using it.

Questions on the intention of use

MARK AN "X" ACCORDING TO YOUR LEVEL OF AGREEMENT	1	2	3	4	5
7. In case I have access to the standards of Information Security practices, I intend to use them.					
8. Considering that I will have access to the Information Security standards, I would use them.					

PART III

(1) Totally disagree – the statement **does not correspond** to my organization's IS policy.

(2) Disagree – the statement **does not correspond in total** to my organization's IS policy.

(3) Neither agree nor disagree – **I do not have** an opinion on my organization's IS policy.

(4) Agree – the statement **partially corresponds** to my organization's IS policy.

(5) Agree – the statement **perfectly corresponds** to my organization's IS policy.

Questions on the agreement related to the adoption

MARK AN "X" IN THE SITUATION THAT IS CLOSEST TO YOUR ORGANIZATION'S	1	2	3	4	5
9. Each network access identifier (or login) is unique for each user.					
10. The network does not accept login of users that are on vacation.					

CC BY

11. The network users commit themselves, in writing, to keep their passwords confidential.					
12. Password reactivation (for users that forgot the password) is made after a strict identification of the user in order to confirm that he or she is really the individual that is requesting the reactivation.					
13. Rights of access to the network are regularly reviewed.					
14. Users are warned not to write their passwords on paper.					
15. Users must regularly change their passwords.					
16. Password input is made by using the mouse.					
17. The procedure for entering the network (or login) is limited to three attempts.					
18. The system of password management forbids reusing passwords.					
19. There are special procedures for using mobile computing resources (e.g., laptops).					
20. When a user leaves the organization, its rights of access are immediately removed.					
21. There is physical control by using biometry in the network usage area.					
22. There are mechanisms for monitoring/recording images of the physical facilities where the network control equipment work.					
23. There are clear rules for holding accountability on the misuse of network resources.					
24. There is some verification on the past of the supposed user of the network in order to check whether he or she has ever infringed any security standards in previous jobs.					
25. New users of the network sign a document stating that they are aware of their responsibility with the information security that will be used in its work.					
26. All users of the network receive proper training for their respective roles on their responsibilities related to information security.					
27. Users that commit errors by security failures are formally held accountable by means of disciplinary processes.					
28. There is a formal procedure for creating a new user and register of your access level.					

CC BY