Article **RINOE Journal**
December 2017 Vol.1 No.1 29-35

The computer security culture reduces the risk of information loss and leakage

RAMIREZ-OCHOA, Dynhora Danheyda*†, BARROSO-BARAJAS, Alfonso José, SIQUEIROS-GARCÍA, Martina Ivonne and VILLAGRAN-VIZCARRA, Dafnis Cain

Universidad Tecnológica de Chihuahua. Montes Americanos 9501, Col del Colegio, 31216 Chihuahua, Chih.

Received July 10, 2017; Accepted December 21, 2017

Abstract

With the accelerated growth of technology we have witnessed the various cyber attacks that can occur to our equipments, due to the threats and vulnerabilities that threaten the security of our equipment and information. This is why it must consider that a computer culture uses the knowledge, skills, attitudes and experience conditioning the activities of personnel to solve their needs and problems through technologies for the storage, processing and transmission of information in a way Automated. The investigation is based on detecting computer security risks through a user-level analysis, applied to the administrative staff of the Technological and Polytechnic Universities in the city of Chihuahua, informing us of the vulnerabilities to which the information is exposed due to the lack of application of Security controls. The results obtained reveal the safety controls required to reduce identified risks.

Computer Security, Computer Culture, Risks, Threats, Vulnerabilities

Citation: RAMIREZ-OCHOA, Dynhora Danheyda, BARROSO-BARAJAS, Alfonso José, SIQUEIROS-GARCÍA, Martina Ivonne and VILLAGRAN-VIZCARRA, Dafnis Cain. The computer security culture reduces the risk of information loss and leakage. RINOE Journal- Schools of economic thought and methology. 2017.1-1:29-35.

* Correspondence to Author (email: dramirez@utch.edu.mx)
† Researcher contributing first author.

1. Introduction

With the accelerated growth of technology, all organizations have based the storage and management of information through the use of technology, which helps in making decisions to strengthen organizations, thus becoming an important asset for them; being necessary to protect it from threats and vulnerabilities that threaten the computer security of Universities.

Given the importance of information, international standardization organizations have developed good practice standards for the safeguarding and good use of information and assets in general. The present investigation makes a diagnosis, based on the IO / IEC 27001 Standard, addressed to the Technological and Polytechnic Universities in the city of Chihuahua; with the interest of applying the best practices in the management of information security. The main objective of the research development is to reduce the identified risks through systematically established procedures. The results obtained allow us to prepare an executive report for the participating Universities, which serves as a support or guide to strengthen computer security at the user level.

1.1 Justification

Information is part of the most important assets of any company and in turn is one of the resources most prone to vulnerabilities, requires its protection against internal and external threats. For this reason, it is necessary to carry out an evaluation to know and apply the computer security controls, which support the staff to enrich their computer security culture, in order to minimize the risks and have the appropriate treatment of data and information.

Norm ISO / IEC 27001: Information Security Management system, provides a quality standard for information security, helping to minimize the risks of damage, theft or leakage of information; allowing to maintain the integrity, confidentiality and availability of the information, in addition to guaranteeing the authenticity of it.

The development of the computer security analysis is based on the ISO / IEC 27001 standard, which allows knowing the existing vulnerabilities in the handling of physical information, as well as that which is contained in the information processing systems, in such a way that preventive and corrective actions can be taken within the organization, to avoid compromising confidential data.

1.2 Problem

Although the Universities have an area or department of systems which is in charge of computer security and to keep their operations stable, it is considered of the utmost importance the awareness and training of the personnel in computer culture which contributes to diminish the related problems with computer security. The lack of knowledge and adequate management of information can harm the organization, which could be vulnerable to any security incident that could damage its operations.

1.3 Hypothesis

The computer security culture of the administrative staff of the Technological and Polytechnic Universities in the city of Chihuahua reduces the risk of information loss and leakage.

ISSN-On line: 2523-6997

RAMIREZ-OCHOA, Dynhora Danheyda, BARROSO-BARAJAS, Alfonso José, SIQUEIROS-GARCÍA, Martina Ivonne and VILLAGRAN-VIZCARRA, Dafnis Cain. The computer security culture reduces the risk of information loss and leakage. RINOE Journal- Schools of economic thought and methology. 2017.

1.4 Objectives

1.4.1 General Objective

Reduce security risks through a computer culture to ensure the confidentiality, integrity and availability of information.

1.4.2 Specífic Objectives

- Determine if the employees know the security policies to safeguard the information of the universities.
- Analyze security vulnerabilities that may exist in the handling of information and systems that affect the continuity of the University's operations.
- Know the current situation regarding the subject of computer security within the University.
- Establish awareness mechanisms for staff on information security issues.
- Process the data obtained from the computer security assessment applied to the Technological and Polytechnic Universities in the city of Chihuahua, for the preparation of a technical report with the analysis and recommendations of computer security.

2. Theoretical framework

Currently the technology has improved a lot of activities for the human being and in some cases the human personnel has been replaced by machines, this entails a risk in which unauthorized persons have access to confidential information and can make bad use of it.

Along with the technological advances that have been generated there has been the concept of computer security which aims to preserve and safeguard damage, alteration or subtraction to the computing resources of an organization and to manage the risk when guaranteeing, in the greater possible measure, the correct uninterrupted operation of those resources; which is achieved through the implementation of a group of controls regulated by standards, procedures, methods, techniques and software and hardware systems aimed at achieving a secure and reliable information system (Aguilera López) (Voutssas M., 2010) .

So it is of utmost importance that any person who has contact with any equipment or technology is instructed in a culture of computer security having a sense of responsibility, respect, ethics and compliance with the rules and policies defined by the organization and society; that, in the long run, guarantees the confidentiality, integrity and availability of the information.

That is why this research aims to emphasize in explaining the why, the when and how of security, creating a culture of security, inculcating awareness of the knowledge, which are currently essential, to properly perform the work of people who use computer tools and work with data and information (Parra Moreno, 2012). Since an informed, trained and educated person will understand why certain standards are dictated and why it is necessary to comply with them, and not only for the sole reason that someone has said it, because it is written, or worse, because.

3. Methodology

The project is based on the field research modality, since it is necessary to resort to the Universities to collect data and perform an analysis with said information.

ISSN-On line: 2523-6997

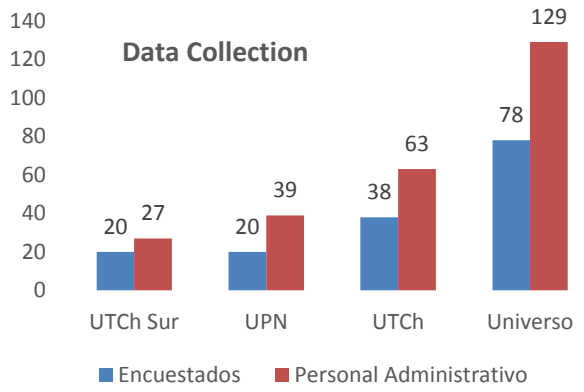
3.1 Type of research

For this research, the following types of research are used:

1. Hypothetical-deductive: which aims to prove that a computer culture can reduce the security risks in a company.
2. Field: since it is based on the information obtained from the administrative staff.
3. Descriptive: Since it details the processes that are carried out and those that are planned in the object of study.

3.2 Population and sample

The universe is made up of the administrative employees of the Technological and Polytechnic Universities in the city of Chihuahua, and in the sample information of 60% of said population was collected.



Graph 1 Population and sample

3.3 Information collection plan

The research techniques used for the collection of information is that of the questionnaire, in which a diagnostic assessment of the knowledge of the user of the computer security that has been implemented in the university is carried out, as well as the planning and the current situation in which are the computers to which the administrative staff have access.

Questions to determine staff knowledge:

1. Do you know who is responsible and the area in charge of computer security?
2. Do you have an antivirus installed on the computer equipment you use?
3. Do you have access to the advanced settings of your computer, such as the control panel?
4. What type of operating system do you use?
5. What services and systems do you consider most critical in terms of availability?
6. Is there equipment that provides uninterrupted power to computers?
7. Do you know how to detect an intrusion or attack on your computer?
8. Approximately how much information you handle is restricted or confidential access?
9. Are there restricted areas in the company that can only be accessed by authorized personnel?
10. What kind of access security tools have you implemented in the company?

Questions to know the computer security plans that are implemented in the University and are basic knowledge:

1. Do you have access to the advanced settings of your computer, such as the control panel?
2. Is there equipment that provides uninterrupted power to computers?
3. Can you download multimedia files from the internet (music, movies, programs, etc.)?
4. Do you have a block to access websites?
5. How many trainings have you had on IT security issues in the last year?
6. Do the passwords you use have combinations of number, uppercase, lowercase, symbols, letters and is more than 10 characters?

ISSN-On line: 2523-6997

7. Is blocking or logout used on the assigned computer?
8. Approximately how much information you handle is restricted or confidential access?
9. Are there restricted areas in the company that can only be accessed by authorized personnel?
10. What kind of access security tools are implemented in the company?
11. How often is the software checked for or updated for viruses, worms, Trojan horses and unauthorized or pirated software?
12. Is there periodic maintenance on the computer equipment?
13. How often do you perform maintenance on computer equipment?
14. Do you allow your operating system to perform the corresponding updates?
15. Is Internet access in the company limited by?
16. Do you require a password to access the WIFI connection?
17. Have the services and systems of the previous list always been available?

Questions to know the current situation of some basic security points:

1. Which of the following computer security incidents have occurred in your workplace in the last year?
2. Do you use computer equipment?
3. Have you had to do your work more than once on your computer due to failures?
4. In what way do you carry out your information backups?
5. In order to install some software to your company computer, do you need support from the personnel of the systems area?
6. Can you download multimedia files from the internet (music, movies, programs, etc.)?
7. Do you have a block to access websites?

4. Results

Derived from the surveys made to the personnel of the universities, the following information is obtained:

– 74.36% use the computer equipment assigned in the company, 57.69% use some confidential or restricted access information and 46.51% use the USB memory to carry out information backups.

– 70.51% have an antivirus installed on their computer, but 64.10% do not know how often that software is updated.

– 89.87% use a Windows operating system, but 28.21% occasionally allows the corresponding updates and 29.49% does not have the habit of updating.

– 57.35% consider that the services offered by the university are always available, 26.04% consider that the academic systems are those that should always be available, but 18.75% did not answer the question.

– 37.18% say they know how to detect an intrusion or attack on their computer, but 98.72% of the staff has not had training in IT security issues.

– 83.33% use a computer with lock for closing session and 61.54% handle secure passwords.

– 52.56% perform maintenance on computer equipment, but 14.03% do not remember how often they do it.

– 53.16% do not know if they have limited internet access, 53.85% of the staff can download multimedia files from the internet.

ISSN-On line: 2523-6997

- 50% have a block to access websites and require a password to access the WIFI connection.
- 69.23% of the personnel knows the responsible person, their position and the area in which they are responsible for security.
- 89.74% of the staff is aware that there are restricted areas where only authorized personnel have access. And 48.84% recognizes the use of fingerprint reader as a security measure.
- 92.31% requires the support of personnel in the systems area to install some software on their equipment and 42.31% have access to the advanced settings of their computer.
- 56.41% almost never had to perform more than once on their equipment due to equipment failure.
- Among the most frequent incidents occurred the computer (21.84%) and other very specific (34.48%).

5. Conclusions

With the investigation it can be observed that the majority of the staff uses the computer equipment, but they do not have enough training to protect and store your equipment and the information that it handles and there are very few that can detect a virus or unauthorized access.

The vast majority is aware that it has an antivirus installed and the type of operating system it works with, but it does not have the habit of updating. The universities have restricted access and with limitations in the use of connections (Internet and WIFI), as well as for the installation of programs; so it is seen that they have a security plan, but even 40% of the staff does not know the restrictions.

In the reports that were delivered in the universities, it was recommended to update and / or carry out security policies, provide courses and training workshops for personnel in which they are informed about computer security, from basic to advanced, depending on the type of information which manages the personnel to be trained.

Therefore, it is affirmed that while the personnel of the Technological and Polytechnic Universities in the city of Chihuahua do not have a computer security culture, there is an increased risk of information loss and leakage, due to ignorance or lack of custom in carrying out the good computer security practices.

6. References

Areitio Bartolin, J. (2008). *Seguridad de la información: Redes, informatica y sistemas de información*. (S. PARANINFO, Editor, M. España, Productor, & Universidad de Deusto) Recuperado el 07 de Febrero de 2017, de Fundamentos de seguridad de la información:áreas de proceso, objetivos, servicios y políticas de seguridad: https://books.google.com.mx/books?hl=es&lr=lang_es&id=_z2GcBD3deYC&oi=fnd&pg=PR14&dq=Cultura+de+seguridad+inform%C3%A1tica&ots=wrpoAFEXNl&sig=SHYuHuDjTrePYDUd_F89anZv0#v=onepage&q=Cultura%20de%20seguridad%20inform%C3%A1tica&f=false

Aguilera López, P. (s.f.). *Seguridad informática*. (S. EDITEX, Editor) Obtenido de https://books.google.com.mx/books?hl=es&lr=lang_es&id=Mgvm3AYIT64C&oi=fnd&pg=PA1&dq=seguridad+inform%C3%A1tica&ots=PprpVBFGZ_&sig=6OeGq3wLXyImkxX8m23k4vvJ8ro#v=onepage&q=seguridad%20inform%C3%A1tica&f=false

ISSN-On line: 2523-6997

Montesino Perurena, I., Baluja García, D., & Porvén Rubier, I. (Ene-abr de 2013). *Ingeniería Electrónica, Automática y Comunicaciones*, versión On-line ISSN 1815-5928. (SciELO, Editor) Recuperado el 09 de Feb de 2017, de Gestión automatizada e integrada de controles de seguridad informática: http://scielo.sld.cu/scielo.php?pid=S181559282013000100004&script=sci_arttext&tlng=pt

Parra Moreno, D. A. (2012). *GESTIÓN DEL RIESGO EN LA SEGURIDAD INFORMÁTICA: "CULTURA DE LA*. Recuperado el 2017 de Febrero de 09, de Ensayo para optar al título de Especialización en Control Interno: http://repository.unimilitar.edu.co/handle/10654/6821

Philco A., M., & Rosero, M. (2014). *publicaciones.usm.edu.ec*. (G. Sansana, Editor) Obtenido de Los riesgos en transacciones electrónicas en línea y la criptografía como modelo de seguridad informática: http://publicaciones.usm.edu.ec/index.php/GS/article/view/44

Voutssas M., J. (Ene-Abr de 2010). *SciElo*, versión impresa ISSN 0187-358X. Obtenido de Preservación documental digital y seguridad informática: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008