redin Revista Facultad de Ingeniería, Universidad de Antioquia, No.89, pp. 81-101, Oct-Dec 2018

MePRiSIA: risk prevention methodology for academic information systems

MePRiSIA: metodología de prevención de riesgos para sistemas de información académica

Isabel Cristina Satizábal-Echavarría[1*] **Nancy María Acevedo-Quintana**[2]

[1]LACSER (Laboratory for Advanced Computational Science and Engineering Research), Universidad Antonio Nariño. Avenida Bolívar # 49 Norte-30. C. P. 630004. Armenia, Colombia.
[2]LOGOS, Universidad de Pamplona. Km 1 vía a Bucaramanga. C. P. 543050 . Pamplona, Colombia.

ARTICLE INFO:

Received: February 08, 2018

Accepted: November 15, 2018

AVAILABLE ONLINE:

November 15 , 2018

KEYWORDS:

Educational information system, information management, information system evaluation, methodology, risk assessment

Sistema de información educativa, gestión de la información, evaluación del sistema de información, metodología, evaluación de riesgos

ABSTRACT: Information of academic systems can be stolen, modified or erased by attackers, causing losses to institutions. Applying a risk prevention methodology at educational institutions would help to avoid academic information misuse by users or attackers. MePRiSIA was designed as a risk prevention methodology to be simple and easy to understand while including the human factor in each step. This methodology has four steps to be considered in the process: setting the context, risk identification, risk analysis, and risk prevention. After being applied to the academic information system of Universidad de Pamplona (Colombia) called ACADEMUSOFT, MePRiSIA was evaluated by experts. In conclusion, after applying MePRiSIA to ACADEMUSOFT, the human factor was part of its most important assets and involved in the very high-level risks identified. According to the experts, implementation of MePRiSIA is hard when institution directors do not provide staff and financial resources for this purpose.

RESUMEN: La información de los sistemas académicos puede ser robada, modificada o borrada por los atacantes y causar grandes pérdidas a las instituciones. Ya que, prevenir es mejor que curar, las instituciones educativas deberían aplicar una metodología de prevención de riesgos para evitar que los sistemas de información académica sean usados incorrectamente por los usuarios o los atacantes. Por ello se diseñó MePRiSIA, una metodología de prevención de riegos simple y fácil de entender que, a diferencia de las existentes, incluye el factor humano en cada paso. MePRiSIA consta de cuatro pasos: establecimiento del contexto, identificación de riesgos, análisis de riesgos y prevención de riesgos. MePRiSIA se aplicó en el sistema de información académica de la Universidad de Pamplona (Colombia) llamado ACADEMUSOFT y fue evaluada por expertos. Después de aplicar MePRiSIA en ACADEMUSOFT, se puede concluir que el factor humano es parte de sus activos más importantes y está entre los riesgos de más alto nivel identificados. De acuerdo con los expertos, la implementación de MePRiSIA es difícil cuando los directivos de la institución no proporcionan el personal ni los recursos financieros para este propósito.

1. Introduction

Currently, educational institutions use information systems to manage academic information such as subjects, grades, schedules, classrooms, etc. However, due to the increasing number of network threats, this information can be stolen, modified or erased by attackers, causing major losses to institutions; for example, Universidad de Pamplona has had multiple lawsuits for possible traffic of grades [1].

Possible causes of this incident are corrupt staff, unauthorized people manipulating the academic information system, users with privileges that do not correspond with their role in the system and improper use of the system because of their lack of knowledge of information security. Thus, people are considered the weakest link in the security chain, but it is necessary to instruct them on better information management practices for the sake of organizations [2]. In [3], Yilmaz and Yalman made a comparative analysis of the security infrastructure of six universities in Turkey. In this analysis, they found that: in the primary defense stage, the main security faults are found in: remote access (50% severely lacking, 33.3% needs improvement), intrusion

* Corresponding author: Isabel Cristina Satizábal Echavarría
E-mail: cristsati@hotmail.com
ISSN 0120-6230
e-ISSN 2422-2844

DOI: 10.17533/udea.redin.n89a11

detection systems (33.3% severely lacking, 50% needs improvement) and wireless (16.7% severely lacking, 83,3% needs improvement); in the authentication stage, the main security faults are: password policies – user account (100% severely lacking), password policies – remote users (100% severely lacking), administrative users (100% needs improvement) and remote access users (50% severely lacking); in the administration and monitoring stage, the main security faults are: secure build (50% severely lacking, 16.7% needs improvement), physical security (50% needs improvement) and event report & response (50% needs improvement). They also found that the main security faults in the people are: policies & procedures (66.7% severely lacking, 16.7% needs improvement) and training & awareness (33.3% severely lacking, 33.3% needs improvement). For this reason, we decided to design a methodology for academic information systems.

Educational institutions should apply a risk prevention methodology to avoid the academic information misuse by users or attackers. Methodologies found in literature are too complex to understand and to carry out, and are focused more on technology than in human factor.

For this reason, a new methodology called MePRiSIA was designed; it is easy to understand while including the human factor in each step. In addition, this methodology is oriented to academic information systems, so it considers the assets of this kind of systems and their vulnerabilities.

The rest of the paper is organized as follows: in section 2, the methodology used to design and evaluate MePRiSIA is described; in section 3, risk prevention and defense in depth model are defined; in section 4, steps of MePRiSIA are described; in section 5, the results of the evaluation of MePRiSIA and its application to ACADEMUSOFT are presented, and conclusions are given in section 6.

2. Methodology

To design the Risk Prevention Methodology for Academic Information Systems (MePRiSIA- **M***etodología de* **P***revención de* **R***iesgos para* **S***istemas de* **I***nformación* **A***cadémica*), the following steps were carried out:

- **Analysis of Risk Management and Prevention Methodologies:** A qualitative approach was used to analyze nine risk management and prevention methodologies found in the literature: OCTAVE [4], CORAS [5], Risk Management Methodology according to Australian Standard [6], NTC-ISO/IEC 27005: Risk Management in Information Security [7], CRAMM [8], MAGERIT [9], Risk Management Guide for Information Technology Systems [10], Methodology for the Diagnosis, Prevention and Control of Corruption in Public Safety Programs according to IDB [11] and Guide to Malware Incident Prevention and Handling [12]. These methodologies were compared to establish similarities and differences among them in [13].

- **Definition of MePRiSIA: Goals and Steps:** From the previous comparison, four steps present in most of the studied methodologies were identified and the distinctive characteristics that MePRiSIA should have. Therefore, the purpose and goals of MePRiSIA as well as the target audience and steps were established.

- **Specification of MePRiSIA Steps:** Reviewing how the studied methodologies carry out the steps established for MePRiSIA, it was determined the most important aspects of each step and the simplest way to obtain the expected results. Taking as a reference the book 'Diseño de un Sistema de Gestión de Seguridad de la Información, Óptica ISO 27001:2005' [14] there were established the fields of the tables and taken into account the requirements of this kind of systems. Thus, the first 3 steps of MePRiSIA were defined. To specify the step 4 of MePRiSIA, the vulnerabilities identified in the assets of step 1 were combined with the 4 elements of the Guide to Malware Incident Prevention and Handling [12], the layers of Defense in Depth model [15], the controls of NTC-ISO/IEC 27001 [16] and knowledge about security measures of the authors.

- **Evaluation of MePRiSIA:** An evaluation form was prepared, and a group of experts were in charge of evaluating and grading the steps of MePRiSIA (from 1(very low) to 5(very high)). They determined if each step is easy to understand, including the human factor and if it is easy to implement. They also had a field to write the observations about each step. Then, the results were analyzed through a matrix that includes: the average value per indicator, standard deviation, weighting per indicator and degree of compliance with goal. The three experts that evaluated MePRiSIA were: Jordi Forné (Ph.D. in Telecommunications Engineering, full professor at the Universitat Politécnica de Catalunya (Spain) and expert in computer security), Rafael Páez (Ph.D. in Telematics Engineering, assistant professor at the Pontificia Universidad Javeriana (Colombia) and expert in computer security) and Rodrigo Alvear (M.Sc. in Management of Computer Projects and technological support coordinator of ACADEMUSOFT).

- **Application of MePRiSIA:** MePRiSIA was applied to ACADEMUSOFT, through a mixed approach. ACADEMUSOFT is an EAS (Enterprise Application Solution) for Higher Education Institutes, created

by the Universidad de Pamplona (Colombia), which allows the management of the academic processes (subjects, grades, schedules, classrooms, personal data of teachers and students, etc.) [17]. This platform is used by several universities in Colombia.

To carry out the first 3 steps of MePRiSIA, the information was obtained from CIADTI staff (Center for Applied Research and Development of Information Technologies) of Universidad de Pamplona, the VII Latin American Survey on Information Security [18] and surveys from students and teachers to determine if they were properly handling the academic information. To calculate the sample size of students and teachers of the seven faculties of the university, Equation (1) was used [19] and the information provided by the Planning Office. The teacher's survey contained 13 multiple-choice questions and the student's survey contains 11 multiple-choice questions.

$$n = \frac{NZ^2pq}{(N-1)E^2 + Z^2pq} \quad (1)$$

Where:
n = Sample size
N = Population size
Z = Confidence level (1.96)
p = Probability of occurrence (0.5)
q = Probability of non-occurrence (q=1-p=0.5)
E = Estimation error (0.05)

Also, CIADTI staff gave access to its test platform to explore the tree of privileges of the users.

To carry out the step 4 in MePRiSIA, the tables established were used, as well as the knowledge about defense in depth model and countermeasures.

3. Background

3.1 Risk prevention

Risk prevention is a continuous process which involves: analyzing current risks in an information system; planning and implementing short and long term activities to avoid or reduce risks that were identified; assessing the effectiveness of such activities and updating them according to changes in the internal and external environment of the institution [20].

3.2 Defense in depth model

To protect organizations against different internal and external threats, is not enough one countermeasure but a set of them to cover the weaknesses and protect the network of possible attacks. Defense in depth model helps in this purpose and includes seven layers [15]:

- **Layer 1 – Policies and procedures:** It is perhaps the most neglected layer, but also the most important, since it provides a guidance to implement the other defenses. Organization must define its most important assets and the level of security that they must have. These policies must be signed by the senior manager and must be known by all the employees and network users.

- **Layer 2 – Physical security:** Since an attacker could damage or steal network devices, it is necessary to establish physical security measures, such as: staff access control, alarm systems, video surveillance, window bars, etc.

- **Layer 3 – Perimeter defense:** The network perimeter is composed of those points of the internal network, managed by the organization, which are in contact with external networks. Firewalls, virtual private networks, border routers that are configured to filter unwanted traffic, are commonly used to defend the perimeter.

- **Layer 4 – Network defense:** Even with the countermeasures installed in other layers, an attacker could gain access to the internal network. To protect the network, it is necessary to use: intrusion prevention and detection systems, network segmentation, IPSec and/or SSL (Secure Socket Layer) to encrypt data, protection of wireless networks, etc.

- **Layer 5 – Equipment defense:** Since an attacker can access to computers of the network, these should be protected, especially the servers. Equipment protection consists of three main tasks: update security patches, disable unnecessary services and maintain the antivirus active and update.

- **Layer 6 – Application defense:** If an attacker gains access to the computer, applications should be protected. In this case, the access to them can be controlled through authentication and authorization mechanisms, and install an application firewall to control the information that they send and receive of the network.

- **Layer 7 – Data defense:** If the attacker crosses all previous defenses, it is necessary that the data stored on the computer is protected, through encryption and integrity mechanisms.

In addition, each of these layers involves the three elements of defense in depth: people, technologies and operations. There must be a balance among these elements so that implemented countermeasures are effective.

4. MePRiSIA design

MePRiSIA is a methodology designed for the Information Technology (IT) staff of educational institutions. This methodology provides a basis for the development of an effective risk prevention program and contains a practical guidance to identify, assess and prevent the risks encountered in an academic information system. MePRiSIA is structured in 4 steps (see Figure 1) that include the human factor. The complete description of MePRiSIA is in [20].

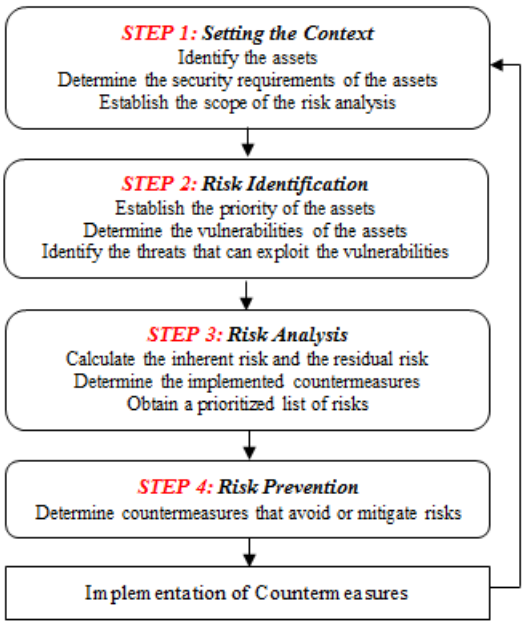

Figure 1 Steps of MePRiSIA

Although, the main vulnerabilities of the assets in an academic information system were identified to give some guidance to the IT staff (tables of step 4), other vulnerabilities can arise from the risk analysis due to the environment of each system.

4.1 Step 1: Setting the context

The goal of this step is to identify the assets of the system, their security requirements and the scope of the risk analysis. To do this, the evaluator must answer the following questions:

1. **What are the assets of the academic information system?** To answer this question, the evaluator must identify the processes carried out by the system, such as visualization of students' academic information (subjects, schedules, and grades), an update of students' grades by teachers, etc. Then, the evaluator must identify the assets involved in each process. The assets commonly found in an academic information system are:

   - **Information:** Assets used to store and manage user information. Within this category are:
     - **Hardware:** Includes the devices of the institution and also those of the users. For example:
       * Servers of the system.
       * Devices used by users to access the system (mobile phones, PCs, laptops, etc.).
     - **Software:** Includes the applications used to make use of the system. For example:
       * Authentication application
       * Database of academic information
       * Web browser or application used by users to access the system
   - **Network:** Includes the communication channel and network devices (switches, routers, etc.). For example:
     - Client/server channel
     - Border router
   - **Staff:** Includes the different users of the system. For example:
     - Students
     - Teachers
     - Administrative staff
     - IT staff
   - **Place:** Includes the places where computers and devices are located. For example:
     - Data center
     - Place where users access the system (internet cafe, home, university).
   - **Organization:** Includes assets that are responsibility of the institution. For example:
     - Image and reputation of the institution.
     - Policies of the system

2. **What is the role of each asset?** To determine the functions that each asset has within the system, according to the identified processes in the previous item.

3. **Which people are responsible for security and management of assets?** To determine who is responsible for each asset, according to the function manuals.

4. **What is the confidential information of the system? and what should be the level of privacy of the information?** First, the evaluator identifies the

personal information that is stored in the system, such as grades of students, financial information, etc. Then, he/she must determine what degree of confidentiality this information should have (low (public information), medium (internal use information), high (confidential information)). Finally, the evaluator must identify the assets that store or transport this information.

5. **What are the security laws that can be applied to the system at a national and regional level?** Government regulations awareness on the management of databases and personal information can be a valuable guideline to manage adequately the system information.

6. **What are the institutional security policies applicable to the system assets?** The evaluator must identify what institutional security policies talk about the assets of the system.

7. **What expectations do the different users have about operation and security of the system?** and if those expectations are defrauded, **what negative consequences would this bring to the good name and reputation of the institution?** To know the expectations of the users and the consequences of defrauding those expectations, the evaluator can do surveys or interviews with a representative sample of each type of user.

In addition, the scope of the risk analysis activities must be defined. According to the budget and the available time, IT staff can decide to focus only on the information and staff assets, or include all the assets. Since people are the weakest link of the security chain [2], staff assets must be included in the analysis.

4.2 Step 2: Risk identification

The goal of this step is to determine the vulnerabilities of the assets and identify the threats that can exploit them by following these steps:

1. **Assets Valuation:** The evaluator must determine the impact a loss of confidentiality, integrity, and availability in each asset can cause on the system and the institution. Ramos Lara [21] states about staff assets valuation that "the operational indicators of human resources are: knowledge, skills, and attitudes". Therefore, for these assets, the evaluator must determine the impact on the system when people do not have the knowledge, skills, and attitudes needed to handle it. A widely used scale to value assets and determine their impact, is the following semi-quantitative Likert scale:

   1: Very Low
   2: Low
   3: Medium
   4: High
   5: Very High

   To determine the impact on each asset, the evaluator must think about the consequences at a functional, economic, legal and administrative level that the loss or lack of these features (confidentiality, integrity, availability, knowledge, skills and attitudes) would bring to the system and the institution, and the time it would take to recover from those losses. Thus, according to the severity of these consequences, the evaluator will give a level in the established scale.

   Table 1 shows the assets valuation table and Table 2 shows the staff assets valuation table. In the two tables, the evaluator must give a value of the previous scale to each feature and put the average of the three values in total column. Next, assets must be ordered from highest to lowest total value and give them a priority (fewer priority to greater total values). If two or more assets have the same value, the evaluator must decide, which of the assets is more important for the system. Thus, the result of this evaluation is a prioritized list of the assets. In prioritizing, the evaluator must include both the staff assets and the other assets in the numbering.

Table 1 Assets Valuation Table

Asset	Availability	Integrity	Confidentiality	Total	Priority

Source: Based on *'Diseño de un Sistema de Gestión de Seguridad de la Información, Óptica ISO 27001:2005'* [14]

Table 2 Staff Assets Valuation Table

Asset	Knowledge	Skills	Attitudes	Total	Priority

2. **Identification of Threats:** A threat is an event that can cause damage to assets. These can have natural or human origin, could be accidental or deliberate, and some of these can affect more than one asset. To determine the threats affecting each asset, the evaluator must ask the responsible for the asset, which incidents have affected the availability or proper functioning of the asset during the last year.

3. **Identification of Vulnerabilities:** The vulnerability is a weakness of an asset. To determine these weaknesses, the evaluator can review the tables

shown in step 4, and look for vulnerabilities that can be exploited by threats identified previously. It is also important to look in literature the most common vulnerabilities of each asset, to determine what privileges different users have and if they are misusing them, how the assets can be damaged.

Table 3 shows the vulnerabilities of each asset and the threats that can exploit them.

Table 3 Identification of Vulnerabilities and Threats

Asset	Vulnerabilities	Threats

4.3 Step 3: Risk analysis

The goal of this step is to establish the level of risk of each threat, determine the implemented countermeasures and obtain a prioritized list of risks. A risk has two factors: its impact and its probability of occurrence. To determine the impact of a risk, the evaluator must take into account criteria such as economic impact, recovery time after the incident, activities or processes of the institution affected by this risk and damage to the image of the institution. According to the severity of these criteria, the evaluator can determine the value of the impact in the following Likert scale:

1: Very Low

2: Low

3: Medium

4: High

5: Very High

To determine the probability of occurrence, the evaluator must ask people responsible of assets about the frequency of each security incident. In addition, taking into account current statistics of recognized sources in security area and the frequency of possible attacks that still have not affected the assets. In this case, it is advisable to use a quasi-exponential Likert scale, where a risk is considered very high when the attack occurs 50% of the time.

0 - 4.99%: 1 Very Low
5 - 14.99%: 2 Low
15 - 29.99%: 3 Medium
30 - 49.99%: 4 High
50 - 100%: 5 Very High

Table 4 shows the fields that the evaluator must fill, using threats identified in Table 3. In addition, the evaluator must calculate the inherent risk, multiplying the impact of risk (IR) and the probability of occurrence (PO) (see Equation (2)).

$$\text{InherentRisk} = \text{IR} * \text{PO} \tag{2}$$

Table 4 Inherent Risk Valuation Table

Asset	Threat	Impact of Risk	Probability of Occurrence	Inherent Risk

Source: Based on *'Diseño de un Sistema de Gestión de Seguridad de la Información, Óptica ISO 27001:2005'* [14]

Then, it is necessary to determine the countermeasures implemented in the system to mitigate each threat. Table 5 shows the fields that must be fill, using threats identified in Table 3. In the third column, the evaluator must describe the countermeasure and in the fourth column, the effectiveness of the countermeasure (EC) must be determine according to the next scale:

0: No countermeasure implemented
1: The countermeasure has not stopped the threat
2: The countermeasure has stopped the threat a few times
3: The countermeasure has stopped the threat several times
4: The countermeasure has stopped the threat most of the time
5: The countermeasure has stopped the threat completely

After that, the evaluator can calculate the residual risk, using Equation (3):

$$\text{ResidualRisk} = \text{PO} * \text{IR}\left(1 - \left(\frac{EC}{5}\right)\right) \tag{3}$$

Table 5 Residual Risk Valuation Table

Asset	Threat	Implemented Countermeasure	Effectiveness of the Countermeasure	Residual Risk	Priority	Risk Level

Next, a risk prioritization is done, ordering the residual risk values from largest to smallest, giving fewer priority to greater risk values. If two or more threats have the same risk value, the evaluator must give the priority according to the importance of the asset determined in Tables 1 and 2 (priority).

Table 6 Definition of Security Policies: Short-Term Controls

Vulnerability	Controls
Lack of security policies for academic information system	• Determine important assets of academic information system. • Put each asset under the responsibility of a particular position or user. • Determine the level of confidentiality of the information stored in the system • Define the level of security that each asset must have. • Determine how each asset must be managed, according to its security level. • Specify the sanctions to be applied when a particular security incident arises. • Determine if security policies are in accordance with information security laws at national and regional level, otherwise make the necessary adjustments. • Determine whether the established security policies are in accordance with institutional security policies, otherwise make the necessary adjustments. • Obtain approval of the policies of academic information system from institution directors.
Lack of information security clauses in employee contracts	• Establish legal contractual terms and conditions related to the confidentiality and security of the information managed by each position.
Lack of responsibilities regarding information security in the description of the positions	• Include in the functions of each position, its responsabilities about security of each asset and the related penalties if the assets are not treated properly. • Verify that these responsibilities are clearly specified in the contract.
Lack of regular audits of academic information system and employees	• Establish the objectives, scope, criteria and frequency of audits to be performed to the assets and staff in charge of them (see in Table 12 "Lack of audit program of academic information system").
Lack of risk identification and risk assessment procedures	• Develop procedures for risk identification, assessment and analysis.
Lack of formal procedure for the control of ISMS* documentation	• Define a formal procedure for the control of ISMS* documentation.
Lack of a formal procedure to remove users from the system and to review periodically access rights	• Establish procedures for the assignment and removal of access privileges to the different types of users. • Define formal procedures for the periodic review of the access rights of each user to the academic information system.
Lack of sufficient staff and work overload	• Define the profiles of the people to hire, in terms of knowledge and human qualities that they should have. • Perform selection, hiring and training of staff in areas with work overload.
Inadequate hiring procedures	• Redefine the steps to be taken to recruit staff. • Define correctly the profiles of the people to hire, in terms of knowledge and human qualities that they should have.
Corruption	• Conduct periodic audits to employees and their work (see Table 12 and Table 13 "Lack of audit program of academic information system"). • Applying the established sanctions to people who do not do their jobs properly.

*ISMS: Information Security Management System

Table 7 Definition of Security Policies: Long-Term Controls

Vulnerability	Controls
Lack of security policies for academic information system	• Conduct periodic reviews of the security policies, so they fit the internal and external context of the institution.
Lack of regular audits of academic information system and employees	• Conduct periodic audits to the academic information system, the employees and their work (see in Table 13 "Lack of audit program of academic information system").
Lack of risk identification and risk assessment procedures	• Carry out risk identification, assessment and analysis procedures to identify risks still present in the system.
Lack of formal procedure for the control of ISMS* documentation	• Apply the established procedure and document properly the ISMS*.
Lack of a formal procedure to remove users from the system and to review periodically access rights	• Review periodically the access rights of each user to the academic information system.
Lack of sufficient staff and work overload	• Review the functions of each position and determine if they should be redistributed more equitably to avoid overloads. • Make appropriate changes in the definition of functions of different positions.
Inadequate hiring procedures	• Conduct interviews and necessary tests to verify that candidates meet the established profiles. • Properly train new staff before they begin to perform their positions.
Corruption	• Conduct awareness sessions to employees, indicating the sanctions due to misuse of assets (see in Table 8 and Table 9 "Lack of training and security awareness").

*ISMS: Information Security Management System

Table 8 Definition of Awareness Programs: Short-Term Controls

Vulnerability	Controls
Lack of training and security awareness	• Identify the common mistakes that the target user group makes and put at risk the information stored in the academic information system. • Define the goals of the awareness program. • Establish the phases of the awareness program. This awareness should be made from the moment the person enters to the institution and then periodically activities must be carried out to reinforce and update knowledge. • Obtain approval and funding for the program from the institution directors. • Select the themes of awareness program. Among these themes are: laws of information security, importance of each type of user in the security chain, precautions that must be taken before, during and after access to the academic information system, minimum security characteristics of the password, etc. • Define strategies and activities to develop the different themes of the program. • Elaborate the material that will be used in the awareness activities. • Train staff responsible to carry out the awareness program.
Incorrect perception of system security by users	• Explain properly to users, from the first time they enter the system, how the implemented security measures work and what role they play in the security chain.

Finally, the evaluator must determine the risk level, with the scale:

1 to 4: Very Low
5 to 9: Low
10 to 14: Medium
15 to 19: High
20 o 25: Very High

4.4 Step 4: Risk prevention

The goal of this step is to determine countermeasures that avoid or mitigate risks.

The evaluator must consult Table 3 to determine which vulnerability corresponds to the threat evaluated in Table 5 and find out each vulnerability in the tables of this section, in order to define the short and long term controls to be planned and implemented.

According to [10], the elements to be considered to propose risk prevention strategies are policies, awareness, mitigation of vulnerabilities and mitigation of threats. For that reason, this step is divided in those parts.

Policies

The following activities can be done to prevent risks arising from the lack of policies:

- **Definition of Security Policies:** These policies define the guidelines to ensure the security of the system assets.
  - **Product:** Security Policies of the Academic Information System.
  - **Main actors:** IT Staff, Institution Directors
  - **Short-term controls:** See Table 6
  - **Long-term controls:** See Table 7

Awareness

The activities that can be carried out to prevent the risks caused by lack of awareness are:

- **Definition of Awareness Programs:** A different program must be defined for each user group, since the degree of depth and specialization of each program will change depending on the role and privileges of these users.
  - **Product:** Awareness Programs for Students, Teachers, Administrative Staff and IT Staff.
  - **Main actors:** Institution Directors, People in Charge of Awareness, Students, Teachers, Administrative Staff and IT Staff
  - **Short-term controls:** See Table 8
  - **Long-term controls:** See Table 9

Table 9 Definition of Awareness Programs: Long-Term Controls

Vulnerability	Controls
Lack of training and security awareness	• Perform awareness activities. • Deliver the material prepared for the different activities. • Monitor the awareness program. • Document and evaluate the results of the awareness program. • Make the appropriate changes to the awareness program.

- **Dissemination of Security Policies:** Ensure that different user groups know the security policies, their responsibilities and the sanctions that would be applied in case of non-compliance.
  - **Product:** Strategies for Disseminating Security Policies to Students, Teachers, Administrative Staff and IT Staff.
  - **Main actors:** Institution Directors, Policy Makers, Students, Teachers, Administrative Staff and IT Staff.
  - **Short-term controls:** See Table 10
  - **Long-term controls:** See Table 11

Mitigation of vulnerabilities and threats

This section takes into account the layers of Defense in Depth Model [15]. The activities that can be carried out to prevent the risks posed by vulnerabilities and threats are:

- **Coordination of Security of the System:** Ensure that all activities for managing the security of the assets and the documentation of the ISMS are carried out according to established security policies.
  - **Product:** ISMS documentation, Security Incident Reports, ISMS Procedures and Action Plans, Audit Reports.
  - **Main actors:** IT Staff, Institution Directors, Audit Team
  - **Short-term controls:** See Table 12
  - **Long-term controls:** See Table 13

Table 10 Dissemination of Security Policies: Short-Term Controls

Vulnerability	Controls
Lack of disclosure of security policies of the academic information system	• Assign creation and implementation of dissemination strategies to a specific position or area. • Establish which security policies apply to each user group. • Define the strategy for the dissemination of security policies to each user group. • Obtain the approval and financing of the diffusion strategies from institution directors. • Develop the material that will be used to disseminate policies.

Table 11 Dissemination of Security Policies: Long-Term Controls

Vulnerability	Controls
Lack of disclosure of security policies of the academic information system	• Carry out activities to disseminate security policies to each user group. • Monitor dissemination strategies. • Document and evaluate the results of dissemination strategies. • Make the appropiate changes in the dissemination strategies.

- **Physical security:** Seeks to protect the places where the assets are located.
  - **Product:** Physical Security Measures
  - **Main actors:** IT staff, Maintenance and Cleaning Staff, Teachers, Students, Administrative Staff.
  - **Short-term controls:** See Table 14
  - **Long-term controls:** See Table 15
- **Perimeter Defense:** Seeks to protect the network perimeter
  - **Product**: Perimeter Security Measures
  - **Main actors:** IT Staff
  - **Short-term controls:** See Table 16
  - **Long-term controls:** See Table 17

Table 12 Coordination of Security of the Academic Information System: Short-Term Controls

Vulnerability	Controls
Lack of security measures in the assets of the academic information system	• Specify the security measures to be implemented in each asset. • Commit the institution directors to support the implementation of these security measures.
Lack of formal security incident handling procedures	• Establish the procedure to report the security incidents of the assets. • Define the action plans that will be implemented when security incidents occur and the maximum response time to each incident. • Establish how security incidents should be documented.
Lack of audit program of the academic information system	• Specify the audit program to be carried out to supervise the assets and the staff in charge of them. • Assign responsibilities to the audit team. • Train the audit team. • Establish the audit schedule.

- **Network Defense:** Seeks to protect information while traveling on the network
  - **Product:** Network Security Measures
  - **Main actors:** IT Staff
  - **Short-term controls:** See Table 18
  - **Long-term controls:** See Table 19
- **Equipment Defense:** Seeks to protect equipment of the system
  - **Product:** Equipment Security Measures
  - **Main actors:** IT Staff, Teachers, Students, Administrative Staff
  - **Short-term controls:** See Table 20.
  - **Long-term controls:** See Table 21.

Table 13 Coordination of Security of the Academic Information System: Long-Term Controls

Vulnerability	Controls
Lack of security measures in the assets of the academic information system	•Implement security measures in each asset. •Monitor security measures of each asset.
Lack of formal security incident handling procedures	• Report security incidents of system assets. •Perform incident recovery activities. •Document security incidents. •Analyze security incidents and determine their probability of occurrence. •Make the appropriate changes in the security measures of each asset to avoid future incidents.
Lack of audit program of the academic information system	•Implement the audit program. •Document audit activities. •Analyze the information obtained in the audit activities to identify the vulnerabilities still present in each asset. •Evaluate the conformity of the audit program with the timetable and established objectives. •Evaluate the performance of the audit team members. •Make the necessary adjustments to the audit program and the audit team.

- **Application Defense:** Seeks to protect applications related to the system
  - **Product:** Application Security Measures
  - **Main actors:** IT Staff, Teachers, Students, Administrative Staff
  - **Short-term controls:** See Table 22
  - **Long-term controls:** See Table 23
- **Data Defense:** Seeks to protect data stored on computers related to the system
  - **Product:** Data Security Measures
  - **Main actors:** IT Staff, Teachers, Students, Administrative Staff
  - **Short-term controls:** See Table 24
  - **Long-term controls:** See Table 25

5. Results and discussion

5.1 Evaluation of MePRiSIA

After MePRiSIA was designed, three experts were in charge to assess the methodology. Table 26 shows the matrix with the results of the evaluation. This matrix includes: the grade given to each indicator by each expert, the average of the grades of each indicator, the standard deviation, the weighting of each indicator according to its importance, the reached value (reached value =(average x weighting)/5), and the degree of compliance (degree of compliance =(reached value x100)/weighting). The scale used for the degree of compliance was:

0% - 69.99% : Low
70% - 89.99%: Medium
90% - 100% : High

According to Table 26, the degree of compliance was higher for steps 1 and 3 than for steps 2 and 4. In addition, in step 1, the degree of compliance of the indicator "easy to implement" is 80% (standard deviation: 1.73), because expert 1 gives a grade of 2, since institutions do not allocate resources for risk prevention.

In step 2, the degree of compliance of indicator "easy to understand" is 80% (standard deviation: 1) because expert 2 gives a grade of 3, since it is unclear how staff assets should be assessed. Also, the degree of compliance of indicator "easy to implement" is 80% (standard deviation: 1) because expert 1 gives a grade of 3, since institutions must have a group of experts to carry out this step.

In step 3, the degree of compliance of the indicator "easy to implement" is 80% (standard deviation: 1), because expert 1 gives a grade of 3, since institutions must have experts in risk management to carry out this step. Finally, in step 4, the degree of compliance of the indicator "easy to implement" is 73.33% (standard deviation: 1.53), because expert 1 gives a grade of 2, due to the little investment in security and the lack of commitment of the institution directors with this issue.

To solve the problem of the indicator "easy to understand" of step 2, this step of the methodology was explained better in [20]. In regards to the commentaries of expert 1 about indicator "easy to implement" of steps 1 and 4, it is true that institutions must allocate resources for risk prevention and directors must be aware of the importance of this issue.

Table 14 Physical Security: Short-Term Controls

Vulnerability	Controls
Location in an area susceptible to flooding and natural disasters	•Make information backups. •Have a contingency plan.
Sensitivity to electromagnetic radiation	•Put equipment in a place where strong electromagnetic radiation does not occur.
Lack of air conditioning	•Put air conditioning in the place where equipment is located.
Susceptibility to moisture, dust and dirt	•Check that the place where equipment is located has not any type of moisture that could affect it.
Unstable electric network	•Verify that the electrical installation of data center has enough power and is in good condition to support different equipment. •Connect equipment through a regulator to the electric network. •Purchase UPS for servers, so they do not stop their operation when there are power outages.
Lack of contingency plan	•Make a contingency plan for data center, in order to know how to deal with unexpected incidents or failures.
Lack of access control to the data center	•Install safety bars in windows. •Put equipment far from windows. •Control the access to the data center, so that only authorized people can access it.
Lack of physical security in the places where the academic information system is consulted	•Take safety precautions when accessing the system, so not exposing the password and avoiding snooping. •Do not forget to close the session of the academic information system. •Erase navigation tracks from computer before leaving.

Table 15 Physical Security: Long-Term Controls

Vulnerability	Controls
Location in an area susceptible to flooding and natural disasters	•Relocate equipment in an area no susceptible to flooding and natural disasters.
Lack of air conditioning	•Perform periodic maintenance to air conditioning.
Susceptibility to moisture, dust and dirt	•Frequently clean the area where the equipment is located and periodically clean the equipment.
Unstable electric network	•Perform periodic maintenance to the electrical installation of data center.
Lack of contingency plan	•Review the contingency plan periodically to make improvements. •Publish the contingency plan to the IT staff responsible for the data center.
Lack of access control to the data center	•Verify the effectiveness of each physical security measure implemented and make necessary changes. •Install a video surveillance system to visualize who access the data center.
Lack of physical security in the places where the academic information system is consulted	•Find a place that provides better security conditions to access the academic information system.

With respect to commentaries of expert 1 about indicator "easy to implement" of steps 2 and 3, although IT staff must have some knowledge about risk management and security to apply MePRiSIA, the most important is the knowledge of the assets and their vulnerabilities, so they should document the different security incidents of the system when they happen, although this is one of the most neglected aspects.

Table 16 Perimeter Defense: Short-Term Controls

Vulnerability	Controls
Unprotected public network connections	•Install a firewall on the network perimeter. •Determine the rules that must be configured to control in and out traffic of the institutional network. •Configure correctly the traffic control rules in the firewall. •Install and configure an intrusion detection system (IDS) integrated with the firewall. •Install and configure an SNMP server that allows monitoring the link with the ISP (Internet Service Provider) and the firewall.

Table 17 Perimeter Defense: Long-Term Controls

Vulnerability	Controls
Unprotected public network connections	•Observe constantly traffic of the ISP link and firewall. •Review constantly logs of the SNMP server. •Analyze the information provided by the SNMP server and obtain statistics. •Periodically check the effectiveness of the firewall and IDS. •Make necessary changes to the firewall, IDS, and SNMP server.

Table 18 Network Defense: Short-Term Controls

Vulnerability	Controls
Unencrypted information traveling through the network	•Encrypt the information with some secure protocol, such as SSL/TLS.
Inadequate network management	•Hire the necessary bandwidth for the academic information system, according to the volume of traffic. •Make the necessary changes in the physical topology of the network to isolate the traffic of the academic information system from the rest of the network. Make this traffic passes through high-speed links and through devices that do not cause bottlenecks.

Table 19 Network Defense: Long-Term Controls

Vulnerability	Controls
Inadequate network management	•Observe in a constantly basis the servers, network devices and links of the main traffic of the academic information system, with an SNMP server. •Analyze the information provided by the SNMP server and obtain statistics. •Make the necessary changes in the servers and in the network to solve the detected problems.

5.2 Application of MePRiSIA

MePRiSIA was applied to ACADEMUSOFT, the academic information system of Universidad de Pamplona (Colombia).

In step 1, there were identified 8 processes and the assets involved in each of them. Table 27 shows the 15 useful assets indicated by MePRiSIA, their functions, and the responsible of each asset.

In addition, personal data of teachers, students, and academic information must have a high level of privacy. Law 1581 of 2012 [21], must be taken into account because it regulates the usage of personal data of users. Finally, a risk analysis was made by including the 15 assets involved in the processes.

In step 2, as proposed by MePRiSIA, the Likert scale was used. Knowledge of the system and its context were used to fill Table 1 and Table 2. Table 28 and Table 29 show examples of the given values and their explanation, and then it was calculated the average of the three values to obtain the total and determined the priority of each asset. Table 27 shows the priority of each asset in the last column, and 2 of the 5 most important assets are part of the staff.

Filling Table 3, there were found 80 vulnerabilities and threats throughout all the assets. Table 30 shows how to do this, by using the vulnerabilities included in tables of

Table 20 Equipment Defense: Short-Term Controls

Vulnerability	Controls
Lack of periodic replacement schedule	•Plan periodic replacement of equipment. •Make periodic information backups.
Multiple people access and share the equipment	•Create user accounts on the computer. Note: The number of people with access permissions to the servers must be small. •Conduct awareness and training sessions for users of the academic information system on security measures for equipment (see in Table 8 and Table 9 "Lack of training and security awareness").
Lack of strong administrator password	•Configure a secure password for administrator account. Note: The administrator password must be known only by one person.
Lack of session termination when computer is abandoned	•Configure the computer to automatically lock after one minute of inactivity and request the password to be unlocked. •Conduct awareness and training sessions for users of the academic information system on security measures for equipment (see in Table 8 and Table 9 "Lack of training and security awareness").
Lack of system restore points	•Insert restore points into the system each time changes are made to the installation or configuration of the computer.
Uncontrolled copy of server information	•Store backup copies in a safe place. •Limit the number of people with access permissions to the server and its backups.
Lack of periodic review of server logs and monitoring the system to detect faults and security incidents	•Check the server's logs daily to detect possible faults and security incidents.
Susceptibility to voltage variations	•Connect the equipment to electric network through a regulator.
Uncontrolled download and installation of free software	•Create user accounts on the computer, so that there is only one administrator with permissions to install programs. Standard user or guest accounts must be used to connect to the Internet, never the administrator account. •Install a good antivirus on the computer. •Update antivirus daily. •Properly install and configure an application firewall on the computer. •Conduct awareness and training sessions for users of the academic information system on security measures for equipment (see in Table 8 and Table 9 "Lack of training and security awareness").
Insufficient maintenance	•Make periodic information backups •Conduct awareness and training sessions for users of the academic information system on security measures for equipment (see in Table 8 and Table 9 "Lack of training and security awareness").
Lack of adequate cooling conditions	•Check if the fans of the equipment are working properly, otherwise clean them or see if there is a mistake in their connection.

Table 21 Equipment Defense: Long-Term Controls

Vulnerability	Controls
Lack of periodic replacement schedule	•Replace equipment according to the schedule.
Lack of system restore points	•Restore the system in case of any operating system damage.
Insufficient maintenance	•Conduct periodically maintenance of software and hardware of the computer.
Lack of control of the changes made in the server configuration	•Document properly changes in server configuration.
Lack of strong administrator password	•Change periodically the administrator password with a password that meets the security features.
Susceptibility to voltage variations	•Connect the server to an UPS so it does not stop operating when there are power outages.
Lack of adequate cooling conditions	•Put air conditioning in the place where the equipment is located.

Table 22 Application Defense: Short-Term Controls

Vulnerability	Controls
•Lack of strong authentication mechanism, lack of complex passwords, and no limit of authentication attempts	•If user/password authentication is used, enable password directives: the user must use a wide set of characters (uppercase, lowercase, numbers, symbols), the password must have a minimum number of 8 characters, there must be a password history, the password must be changed after a certain number of days and the accounts must be blocked after a certain number of failed attempts.
•Lack of session termination when computer is abandoned	•Configure services so that user sessions are terminated after several minutes of inactivity. •Conduct awareness and training sessions to users about the correct use of the academic information system (see in Table 8 and Table 9 "Lack of training and security awareness").
•Uncontrolled copy of server information	•Ensure that only a limited number of authorized people have access to the server and its backups.
•Lack of confidentiality of access password to academic information system **•Lack of security precautions when accessing the academic information system** **•Lack of browser settings regarding: cookie blocking, password storage, security level, history storage, etc.** **•Indiscriminate installation and activation of add-ons**	•Conduct awareness and training sessions to users about the correct use of the academic information system (see in Table 8 and Table 9 "Lack of training and security awareness").
•Incomplete or unclear specifications for developers	•If the system is proprietary, complete software documentation, so that it is understandable to developers.
•Failures in software design and implementation that create security holes	•Inform developers about faults encountered.
•Complex user interface	•Train users on the proper use of the application and its aids.

step 4, the knowledge about the assets, the threats that can exploit those vulnerabilities, and vulnerabilities and threats information found in the literature.

The proposed Likert scale was used in step 3, to grade the impact of risk, taking into account the damages that the threat can cause to ACADEMUSOFT and the institution. Afterwards, CIADTI staff was asked to give

Table 23 Application Defense: Long-Term Controls

Vulnerability	Controls
Lack of strong authentication mechanism, lack of complex passwords, and no limit of authentication attempts	•If academic information system is proprietary, implement a strong authentication mechanism to access the academic information system, involving at least two factors (something you know, something you have, something you are). •Monitor the authentication mechanism. •Analyze the data generated by monitoring the authentication mechanism, in order to determine its effectiveness.
Failures in software design and implementation that create security holes Incomplete or unclear specifications for developers	•If the academic information system is proprietary, when a modification is made to the applications, a software development methodology must be used that takes into account security and that provides good documentation of the changes made. •If the academic information system is not proprietary, failures must be reported to the software creator.
Defects in software and insufficient testing	•If the academic information system is proprietary, after modifications, test the software before making it available to users. •If the academic information system is not proprietary, the defects must be reported to the software creator.
Complex user interface	•If the academic information system is proprietary, develop a user manual of the application, ask users about the difficulties they encounter in using the interface and make the necessary changes in order to reduce its complexity. •If the academic information system is not proprietary, report the difficulties to the developers.

Table 24 Data Defense: Short-Term Controls

Vulnerability	Controls
Storage without proper protection of academic information	•Back up the information. •Store information encrypted. •Keep the information storage device under surveillance so it is not stolen.
Lack of backups	•Make daily backups of important information.
Lack of confidentiality of the information that downloads from the academic information system	•Conduct awareness and training sessions for users of the academic information system on security measures for information (see in Table 8 and Table 9 "Lack of training and security awareness"). •Store information encrypted. •Keep the information storage device under surveillance so it is not stolen.
Storage of passwords unprotected	•Save user passwords encrypted in the database and other devices.
Entering storage devices on unprotected computers **Neglect of the place where the storage devices are left** **Lack of backups of storage devices**	•Conduct awareness and training sessions for users of the academic information system on security measures for information (see in Table 8 and Table 9 "Lack of training and security awareness").

Table 25 Data Defense: Long-Term Controls

Vulnerability	Controls
Storage without proper protection of academic information	•Verify the integrity of stored information when necessary. •Use backups to recover information in case of damage or theft.
Lack of backups	•Use backups to recover information in case of damage.

the probability of occurrence of each threat, according to the quasi-exponential Likert scale of step 3. In some cases, it was necessary to use the results of the VII Latin American Survey on Information Security[[18] if the CIADTI staff did not give an specific value. To find out students and teachers threats, the results of the surveys carried out in the institution were valuable. Then, by multiplying the impact of risk, and the probability of occurrence it was obtained the inherent risk (see Table 31).

Table 26 Matrix of Evaluation

Steps and Indicators	Expert 1	Expert 2	Expert 3	Avereage	Standard Deviation	Weighting	Reached Value	Degree of Compliance
STEP 1: Setting the Context						20%	19%	95%
Easy to understand	5	5	5	5	0	8%	8%	100%
Includes human factor	5	5	5	5	0	7%	7%	100%
Easy to implement	2	5	5	4	1.73	5%	4%	80%
STEP 2: Risk Identification						25%	21.33%	85.33%
Easy to understand	4	3	5	4	1	10%	8%	80%
Includes human factor	5	4	5	4.67	0.58	10%	9.33%	93.33%
Easy to implement	3	4	5	4	1	5%	4%	80%
STEP 3: Risk Analysis						25%	23.33%	93.33%
Easy to understand	4	5	5	4.67	0,58	10%	9.33%	93.33%
Includes human factor	5	5	5	5	0	10%	10%	100%
Easy to implement	3	5	4	4	1	5%	4%	80%
STEP 4 : Risk Prevention						30%	26.67%	88.89%
Easy to understand	4	5	5	4.67	0.58	10%	9.33%	93.33%
Includes human factor	5	5	5	5	0	10%	10%	100%
Easy to implement	2	5	4	3.67	1.53	10%	7.33%	73.33%

The residual risk and each threat priority were determined, taking into account the priority of each asset (see Table 27) in case of a tie. Finally, it was established the risk level, according to the scale for this purpose in step 3. Table 32 shows an example of the results obtained.

Thus, seven very high-level risks were identified due to: unawareness of security policies of ACADEMUSOFT and lack of training and security awareness by teachers, CIADTI staff and students; lack of confidentiality and complexity of the password of the teachers; lack of a formal procedure to remove users from the system and to review periodically access rights; lack of information security provisions in employee contracts; and lack of security policies for ACADEMUSOFT. Therefore, it is important to create and disseminate complete security policies, as well as awareness and training to users about system security. Therefore, it is important to create and disseminate complete security policies, as well as awareness and training to users about system security.

Since CIADTI staff did not provide all information of ACADEMUSOFT needed, some assumptions were made about the possible vulnerabilities and threats of the assets and their value. It is recommended that the IT staff of each institution carries out this methodology because it has all the information for its development, and it is necessary that somebody knows about information and network security.

In step 4, short-term and long-term controls were determined, according to the tables of step 4. When vulnerabilities did not match those of the tables, the most resembled vulnerabilities were taken as examples to establish the controls, using common sense and security knowledge. Table 33 shows an example of the results obtained.

Finally, CIADTI staff pointed out the difficulty in implementing the controls suggested by the methodology, when the institution does not allocate staff and financial resources for this purpose, which highlights the importance of awareness the institution directors regarding the necessity of these security measures.

6. Conclusions

MePRiSIA is a risk prevention methodology for academic information systems that has four steps: setting the context, risk identification, risk analysis, and risk prevention. In setting the context, the evaluator identifies the assets of the system by process, determines the security requirements of each asset and the information, and establishes the scope of the risk analysis. In risk

Table 27 Step 1: Assets, Functions, Responsible

Asset	Function	Responsible	Priority
HARDWARE			
Server of academic information database and authentication	Hosts academic information database and authentication application of ACADEMUSOFT. Also, it allows users to access to these services.	CIADTI	2
Users' devices	Allow the use of web browser by users to access ACADEMUSOFT.	USERS	14
Storage devices of the users	Store the information that users upload and download from ACADEMUSOFT.	USERS	12
SOFTWARE			
Authentication service	Verifies if username and password are correct, to allow or deny user's access to ACADEMUSOFT.	CIADTI	7
Interface of academic information database	Shows database information and allows its modification and download.	CIADTI	1
Web browser of the users	Allows to display ACADEMUSOFT.	USERS	15
NETWORK			
Client/Server communication channel	Transports information shared between server and users.	CIADTI	8
STAFF			
Students	Can consult and download their grades, schedules, subjects and financial registration, as well as modify their personal data.	STUDENTS	10
Teachers	Can consult and download the lists of their students and the grades of their courses, consult their educational evaluations, update the grades of their courses and modify their personal data.	TEACHERS	6
Administrative Staff	Can introduce certain personal data of the students and teachers, as well as to modify certain academic information.	ADMINISTRATIVE STAFF	4
CIADTI Staff	Can activate/deactivate the privileges of the users and manage the software of ACADEMUSOFT.	CIADTI	3
PLACE			
Data center	Hosts the servers and network devices	CIADTI	5
Place where users consult ACADEMUSOFT	Hosts PCs, laptops, etc. that users use to access ACADEMUSOFT.	USERS	13
ORGANIZATION			
Image and Reputation	Must improve every day so institution can sell ACADEMUSOFT platform to other institutions.	UNIVERSITY	9
Policies of ACADEMUSOFT	To establish the guidelines for the correct functioning of ACADEMUSOFT.	CIADTI AND INSTITUTION DIRECTORS	11

identification, the evaluator establishes the priority of the assets, determines the vulnerabilities of each asset and the threats that can exploit them. In risk analysis, the evaluator, calculates the inherent and residual risks, determines the implemented countermeasures and obtains a prioritized list of risks. Finally, in risk prevention, the evaluator determines the countermeasures that avoid or mitigate the identified risks.

MePRiSIA was designed to be simple and focused on

Table 28 Step 2: Assets Valuation

Asset	Availability	Integrity	Confidentiality	Total	Priority
Place where users consult ACADEMUSOFT	2 (Users have different alternatives, so if one of these places is not available, they can access through other places)	1 (The bad conditions of the place does not affect the access if the device works)	3 (Users should be aware of people who are observing them when entering the campus, because their password and personal information may be compromised.)	2.33	13

Table 29 Step 2: Staff Assets Valuation

Asset	Availability	Integrity	Confidentiality	Total	Priority
Students	3 (The system shows help messages and links to documents about its operation, so students might not require help from others. Students lack knowledge would not impact normal development of academic processes if they access personal information and modify their data.)	4 (If students do not have the skills to manage ICT, they can request help from other people, so their password and personal information can lose privacy)	4 (Lack of precautions when entering the system, or giving the password to other people to consult information are considered bad practices that cause personal information to be exposed.)	3.67	10

Table 30 Step 2. Vulnerabilities and Threats

Asset	Vulnerabilities	Threats
Client/Server communication channel	Unencrypted information traveling through the network	Sniffing
	Unprotected public network connections	Sniffing MITM (Man in the Middle) Remote espionage
	Inadequate network management	Network congestion

the human factor. In step 1, human factor is part of the assets of the system, taking into account staff responsibilities and expectations. In step 2, human factor is included in assets valuation, when evaluating the knowledge, skills and attitudes of staff. This kind of evaluation was not present in other methodologies. In addition, in the identification of vulnerabilities and threats, the staff assets are included, analysing the privileges of the different users in the system to determine if they can be the cause of a security incident. In step 3, the vulnerabilities and threats of the staff assets are part of the analysis. Finally, in step 4, human factor is taken into account mainly in the policies, the awareness programs and the audits.

According to the experts that evaluated MePRiSIA, although this is easy to understand and includes the human factor in each step, it is hard to implement when evaluators do not have knowledge about information security and institution directors do not provide staff and financial resources for this purpose.

After MePRiSIA was applied to ACADEMUSOFT, the conclusion was that human factor is part of its most

Table 31 Step 3: Inherent Risk Valuation

Asset	Threat	Impact of Risk	Probability of Occurrence	Inherent Risk
Server of academic information database and authentication	Expiration of the useful lifetime of the server and its parts	(Hardware damages due to the absence of periodic replacement has a very high impact because the server stops working for a period of time, causing delays in academic processes and sometimes loss of information.)	2 (According to CIADTI staff)	10
Web browser of the users	Impersonation attacks	4 (If a user does not end their session in ACADEMUSOFT before leaving the computer, an attacker can view, modify or delete the information, and this user can accuse the institution unjustly, affecting its image.)	2 (According to the VII Latin American Information Security Survey, the percentage of occurrence of impersonation attacks is 12.7%)	8

Table 32 Residual Risk Valuation

Asset	Threat	Implemented Countermeasure	Effectiveness of the Countermeasure	Residual Risk	Priority	Risk Level
Server of academic information database and authentication	Expiration of the useful lifetime of the server and its parts	None	0	10	40	Medium
Web browser of the users	Impersonation attacks	None	0	8	55	Low

Table 33 Step 4: Short-Term and Long-Term Controls

Asset	Priority	Vulnerability	Controls
Policies of ACADEMUSOFT	5	Lack of a formal procedure to remove users from the system and to review periodically access rights	**SHORT-TERM:** •Establish procedures for the assignment and withdrawal of users' access privileges to ACADEMUSOFT. •Define formal procedures for the periodic review (supervision) of the access rights. **LONG-TERM:** •Periodically review the access rights to ACADEMUSOFT of each user.

important assets and is involved in the very high-level risks identified, therefore it is very important that users know how to use correctly the systems and which information they must protect.

Finally, although MePRiSIA was designed for academic information systems, this methodology can be extended to other types of systems, since the identified assets and the controls can be applied to any system.

7. Acknowledgments

This work was supported by Universidad de Pamplona (Colombia) under *Convocatoria Interna de Mujeres Investigadoras 2014* [number PR130-00-21 (GA 190-CM-I-2014-2.1.2.2.1)].

References

[1] Sistema Informativo de Canal 1. (2013, Oct. 20) Investigan venta de notas y títulos profesionales en universidad de pamplona. Accessed Jun. 12, 2014. [Online]. Available: https://goo.gl/cmuvYR

[2] J. E. L. Rueda. (2013, September) El ser humano: Factor clave en la seguridad de la información. [Online]. Available: http://apuntesdeinvestigacion.bucaramanga.upbbga.edu.co/

[3] R. Yilmaz and Y. Yalman, "A comparative analysis of university information systems within the scope of the information security risks," *TEM Journal*, vol. 5, no. 2, pp. 180–191, 2016.

[4] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, "Introducing OCTAVE allegro: Improving the information security risk assessment process," Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, Tech. Rep. CMU/SEI-2007-TR-012, May 2007.

[5] *The CORAS Model-based Method for Security Risk Analysis*, SINTEF, Oslo, 2006.

[6] *Estándar Australiano, Administración de Riesgos*, AS/NZS 4360:1999, 1999.

[7] *NTC-ISO/IEC 27005: Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información*, ICONTEC, Bogotá, Colombia, 2009.

[8] M. M. Qasem, "Information technology risk assessment methodologies: Current status and future directions," *International Journal of Scientific & Engineering Research*, vol. 4, no. 12, pp. 966–972, Dec. 2013.

[9] *Magerit version 1.0: Risk Analysis and Management Methodology for Information Systems*, 1st ed., Ministerio de Administraciones Públicas, Madrid, España, 1997.

[10] *Risk Management Guide for Information Technology Systems*, National Institute of Standars and Technology, Gaithersburg, 2002.

[11] M. García. (2010) Metodología para el diagnóstico, prevención y control de la corrupción en programas de seguridad ciudadana. [Online]. Available: https://goo.gl/PF1oMo

[12] P. M. Mell, K. Kent, and J. Nusbaum, "Guide to malware incident prevention and handling," National Institute of Standards and Technology (NIST), Gaithersburg, Maryland, Tech. Rep. 800-83, Nov. 2005.

[13] N. Acevedo and C. Satizábal, "Risk management and prevention methodologies: a comparison," *Sistemas & Telemática*, vol. 14, no. 36, pp. 39–58, 2016.

[14] A. G. Alexander, *Diseño de un Sistema de Gestión de Seguridad de Información: Óptica ISO 27001:2005*, 1st ed. Bogotá, Colombia: Alfaomega, 2007.

[15] G. Alvarez and P. P. Pérez, *Seguridad Informática para Empresas y Particulares*. Madrid, España: McGraw-Hill Interamericana, 2004.

[16] *Norma Técnica NTC-ISO/IEC Colombiana 27001. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la información (SGSI). Requisitos*, ICONTEC, Bogotá, Colombia, 2006.

[17] CIADTI. (2017) Academusoft. Accessed Aug. 25, 2017. [Online]. Available: https://goo.gl/yPS97Z

[18] J. J. Cano and G. M. Saucedo, "Vii encuesta latinoamericana de seguridad de la información," ACIS, Bogotá, Colombia, Tech. Rep., Jun. 2015.

[19] M. Badii, A. Guillen, E. Cerna, and J. Valenzuela, "Nociones introductorias de muestreo estadístico," *International Journal of Good Conscience*, vol. 6, no. 1, pp. 89–105, Jun. 2011.

[20] N. M. A. Quintana, "Metodología para la prevención de riesgos en el manejo de la información personal almacenada en el sistema de información académica de la universidad de pamplona," unpublished.

[21] C. de Colombia. (2012, Oct. 17). [Online]. Available: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

[22] K. J. R. Lara, "Sistema de índices para la valoración de los activos intangibles," *Contribuciones a la Economía*, no. 2014-04, July 2014.