applied sciences

MDPI

Article

MASISCo—Methodological Approach for the Selection of Information Security Controls

Mauricio Diéguez [1,*], Carlos Cares [1], Cristina Cachero [2] and Jorge Hochstetter [1]

[1] Departamento de Ciencias de la Computación e Informática, Universidad de La Frontera, Temuco 481-1230, Chile
[2] Departamento de Lenguajes y Sistemas Informáticos, Universidad de Alicante, 03080 Alicante, Spain
* Correspondence: mauricio.dieguez@ufrontera.cl

Abstract: As cyber-attacks grow worldwide, companies have begun to realize the importance of being protected against malicious actions that seek to violate their systems and access their information assets. Faced with this scenario, organizations must carry out correct and efficient management of their information security, which implies that they must adopt a proactive attitude, implementing standards that allow them to reduce the risk of computer attacks. Unfortunately, the problem is not only implementing a standard but also determining the best way to do it, defining an implementation path that considers the particular objectives and conditions of the organization and its availability of resources. This paper proposes a methodological approach for selecting and planning security controls, standardizing and systematizing the process by modeling the situation (objectives and constraints), and applying optimization techniques. The work presents an evaluation of the proposal through a methodology adoption study. This study showed a tendency of the study subjects to adopt the proposal, perceiving it as a helpful element that adapts to their way of working. The main weakness of the proposal was centered on ease of use since the modeling and resolution of the problem require advanced knowledge of optimization techniques.

Keywords: information security management; selection of security controls; security risk; security standards; optimization problem; operational research; intention to adoption

Citation: Diéguez, M.; Cares, C.; Cachero, C.; Hochstetter, J. MASISCo—Methodological Approach for the Selection of Information Security Controls. *Appl. Sci.* **2023**, *13*, 1094. https://doi.org/10.3390/app13021094

Academic Editors: Gianluca Lax and Antonia Russo

Received: 13 October 2022
Revised: 30 October 2022
Accepted: 31 October 2022
Published: 13 January 2023

1. Introduction

Information Security (IS) has gained significant relevance within the work of organizations [1]. In the recent past, there have been reports of serious violations that various organizations have suffered in their systems, which meant losses of hundreds of millions of dollars to the world economy [2].

Little by little, awareness of the latent danger of not considering the minimum aspects of IS within its processes has grown worldwide. As a result, minimizing the risk of attacks through eliminating vulnerabilities has become, in many cases, a priority objective of organizations [2].

This need is transversal to the type of organization, whether a private company or a governmental organization, a large or a small company, as any organization is exposed to malicious attacks that seek to take advantage of any vulnerability [3]. The diversity of attack types forces organizations to take actions that will eliminate any vulnerabilities present or minimize the attack's impact [4].

The above implies that organizations must be constantly alert, generating a proactive defense of their information assets. One way to protect themselves is by implementing best practices to minimize risks [5].

Information security risk management is a process that focuses on the identification and analysis of security risks. These analyses allow the evaluation of potential impacts and the determination of actions to be implemented to reduce such risk [6].

Based on the above, Dubois et al. [7] presented four information security risk management categories:

- Risk Management Standards. It includes standards such as ISO/IEC Guide 73 [8] and AS/NZs 4360 [9].
- Security Requirements Frameworks. Proposals such as, Mellado et al. [10], Khan e Ikram [11], and techniques, such as, SecureUML [12,13] and SIREN [14].
- Risk management methods, such as OCTAVE [15], and CORAS [16].
- Information security standards, such as ISO27001 [17], NIST [18], and COBIT [19].

The proposal is part of the latter approach to risk management. In this sense, IS standards propose this set of good security practices through the implementation of an Information Security Management System (ISMS) [20]. The actions proposed by a standard are transversal to the organization, affecting its organizational structure, policies, technological infrastructure, human resources, and processes, among other areas [3].

While it is true that the standard is clear regarding the implementation of the entire management system, there may be differences concerning partial implementations since organizations have different characteristics and different capabilities and resources [21,22].

Therefore, the decision regarding the progress in achieving the standard is not trivial since it must consider various aspects of the organization, such as risk, costs, implementation times, prioritizations, and policies, among others.

Usually, experts in implementing an ISMS make recommendations for advancement [22,23]. However, this approach is subjective and does not ensure an optimal recommendation, as it does not follow a standardized process with well-defined steps and proven support techniques. Therefore, although this type of recommendation may meet the requirements and characteristics of the organizations, it does not optimize the use of resources.

In this context, it becomes relevant to support decision-making regarding the progress in achieving a standard. However, the multiplicity of factors involved in this process complicates the resolution of the problem. Elements such as risk, cost, time, or human factors, among others [24], transform this problem into a multi-objective problem subject to resource constraints.

Then, the methodological approach proposed in this work defines a systematic and repeatable process supported by mathematical modeling, multi-objective problem-solving techniques, and supported whit computer tools. This approach dramatically supports decision-making, decreasing the decision time, and increasing the recommendation accuracy from the perspective of resource optimization.

Accordingly, the main objective of the investigation is to define a methodology for selecting information security controls that will help security consultants make their recommendations more efficiently, effectively, and with greater satisfaction than they would obtain using their usual methods. To this end, we propose that the methodology be based on a quantitative model for selecting information security controls and that it be supported by software tools that partially automate the process.

As a direct result of this research, the following contributions to the area under study can be listed:

1 Methodological approach for control selection: From the above, the main contribution of this article is the proposal of a methodological approach for the optimal selection of security controls. This approach allows systematizing a process that, to date, is not structured but depends on the criteria of each security expert.
This work defines: (i) stages of the process, (ii) categorizes possible situations that can be faced, (iii) proposes techniques to be applied in each category, and (iv) details the products at each stage of the process.
The advantages of this approach are mainly related to the systematization of the process, the possibility of solving complex recommendation problems, and the reduction of the time required to solve the problem.

2 Proposal evaluation: This paper also evaluates the proposal by applying a methodology adoption study. This empirical study provides relevant information regarding adopting the methodological proposal by a group of new consultants in information security analysis.
In this sense, a tendency towards adopting the proposal by the subjects of the study was evidenced, showing that the proposed model is perceived as a helpful tool for making security investment recommendations. However, the study showed that the design of the optimization model is complex to structure for someone who needs more knowledge in this area.

3 Software tool for control selection: Another significant contribution of this research is the design and development of a prototype software tool that supports the proposal's application. This tool supports the user in all process phases, from information collection to the optimization model's resolution.

2. Materials and Methods

For the development of this proposal, we have applied the research method based on the Design Science paradigm [25]. This paradigm proposes the resolution of practical problems through developing new artifacts that innovate the processes studied [26].

The Design Science research cycle proposes the development of research through 6 phases: (1) problem identification; (2) definition of objectives; (3) design and development; (4) demonstration; (5) evaluation; and (6) communication, as illustrated in Figure 1.

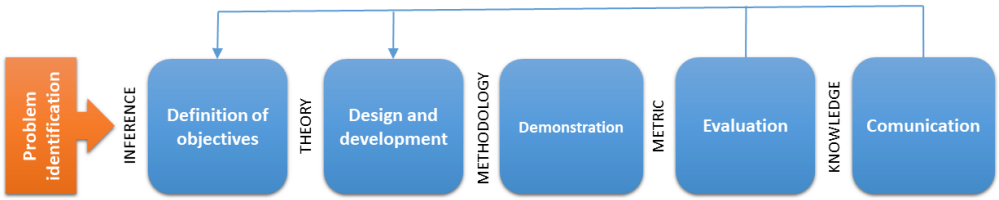


Figure 1. Research Cycle—Design Science [25].

One of the characteristics to consider in this paradigm is the flexibility in the research development since it allows the application of a different methodological framework in each phase, according to the research needs.

In the context of this work, the practical problem that underpins the research refers to the difficulties faced by security consultants in generating recommendations for implementing security controls through an objective and systematic process to optimize the organization's resources.

Considering the above and according to the scope of the research, we adapt the stages of the Design Science paradigm into four phases:

i Problem investigation, where the stages of "Problem identification" and "Objective definition" were developed.

ii Design of the proposal, where we built the methodological approach and identified the techniques and tools, covering the stages of "Design and development" and "Demonstration."

iii Evaluation of the proposal, where the validation framework was defined, including the measurement instruments and the validation process, applied, covering the "Evaluation" stage of the method.

iv The "Communication" stage corresponds to the presentation of the results of the research work.

2.1. Phase 1: Problem Investigation

In this phase, we studied what the literature indicates regarding the process of recommending controls. First, through a Systematic Mapping of the literature, we review the state of the art regarding quantitative models to select controls. In addition, the information

security standard ISO27001:2013 and the guidelines for auditing management systems presented in the ISO19011:2018 standard, were analyzed to determine whether they propose a formal method for recommending security controls.

Secondly, we conducted a literature search in the body of knowledge in the area of Operations Research (OR) to identify quantitative optimization methods that apply to the problem of control selection and thus provide methods to reduce subjectivity in the selection.

The proposals reviewed identify which processes would be part of the proposal and, in addition, determine which processes should be developed to complete the design of the methodological approach and determine the optimization models that will integrate the selection problem.

2.2. Phase 2: Proposal Design

This phase consists of 2 stages: the first is related to the design of the methodological framework, while the second deals with the design and development of a software tool that supports the proposal's application.

In stage 1, based on the information found both in the standards and in the literature review, a methodological framework is designed to cover the deficiencies found and to complement the current way of working (based on expert opinion and therefore subject to a high degree of subjectivity). In addition, it integrates quantitative optimization methods into this proposal to improve the objectivity and traceability of decisions.

In the second stage, a prototype software tool is developed to apply the methodological framework in order to support the expert in (i) capturing and storing the information, (ii) modeling and solving the optimization problem, and (iii) summarizing and visualizing the results.

2.3. Phase 3: Proposal Evaluation

In this stage, we evaluated the proposal's performance by studying the users' perception of the methodological framework. This stage seeks to answer questions such as: What is the perception of the relevant stakeholders about the proposed method? Does the proposed method generate benefits concerning the methods traditionally used? Etc. To study the user's perception, we conducted an adoption study to determine the degree to which users would be willing to change their practices and adopt the proposed methodological framework.

For this evaluation, we apply a quasi-experiment [27] with undergraduate students. The results obtained were used to evaluate the differences in the subjects' perceptions regarding the use of the proposal.

The student's perception of applying the Methodological Framework was evaluated through an adoption intention study. For the analysis, we applied the UMAM methodology adoption model [28], which allows us to study the adoption of a new work method by the users involved through the application of the validated UMAM-Q questionnaire.

3. Results

3.1. Phase 1: Investigation of the Problem

As a first step of the research, we studied several bibliographic sources to determine which processes are currently applied to manage, select or recommend information security controls. We reviewed the scientific literature through a systematic mapping and proposals from industry practice.

To get the look from practice, we reviewed the indications proposed in two standards of the International Organization for Standardization (ISO) (https://www.iso.org/ (accessed on 3 November 2022)). The first one is the ISO/IEC 27001:2013 [17] since it is one of the best-known standards for information security management [29]. The second is ISO/IEC 19011:2018 [30], a guide for developing management system audit processes. This standard proposes several steps to carry out an audit, among which is the definition of an improvement plan, which involves the selection process of controls of a standard.

ISO/IEC 27001:2013 was developed to propose requirements for designing and implementing an Information Security Management System (ISMS). According to this standard, Section 6.1.3, "Information security risk treatment", in point (b) indicates that the organization must determine the controls necessary to implement the information security risk treatment. However, as can be seen, this indication does not provide detailed guidelines on how to make this selection; it only implies that this selection should be consistent with the risk levels identified by the organization. Therefore, it is left to the assessor's discretion to decide how to discriminate from the entire set of controls that allow risk mitigation, those that will allow him to comply with the organization's resource restrictions.

On the other hand, ISO/IEC 19011:2018 is a non-certifiable international standard that establishes guidelines for the audit of a management system. Therefore, this standard does not establish requirements. However, it is a guide that orients the management of an audit program that allows the improvement of the implemented management system, stimulating the incorporation of practices associated with the evaluated management system.

According to Note 2 of point 3.4 of the standard, "Audit findings may lead to identifying opportunities for improvement or recording best practices". Similarly, in point 6.4.8, it is stated that "If the audit plan so specifies, audit findings may lead to recommendations for improvement or future audit activities". From these points, it is clear that the guide states that the audit team, as part of the audit report, may recommend a series of actions that the organization can take to improve the management system.

However, given the generality of the standard, it does not establish a procedure or methodology to guide the audit team on how to determine or select the set of improvements or actions the organization should implement in its management system. Thus, this process, as in the previous case, is left to the discretion and experience of the audit team.

As has been seen, none of the standards reviewed provide guidelines on how to proceed to make recommendations for improvements through implementing security controls. In other words, although both standards recognize the need to move towards improvement by implementing best practices in the work of the ISMS, neither provides formal guidelines on how to select the best actions to implement, leaving this process to expert judgment.

To evidence the proposals in the literature regarding the application of methods or techniques to select and schedule the optimal set of information security controls, we analyze the results of a systematic mapping performed in [31].

Table 1 summarizes the proposed control recommendation methods classified according to, on the one hand, the complexity of the problem addressed: (i) Prioritization, as an ordered list of security controls but without selecting a subset of these; (ii) Selection of controls, where the models recommend a specific set of controls to implement; (iii) Programming, where in addition to selecting controls, the model proposes a plan for the implementation of these controls. On the other hand, the methods are classified between (a) quantitative solutions, i.e., mathematical models where at least one objective function exists and some known optimization algorithm is executed, and (b) qualitative solutions.

Table 1. Classification of proposals according to the complexity of the problem and the use of quantitative techniques.

Category	Solution Type	
	Quantitative Solutions	**Qualitative Solutions**
Prioritization		9 papers—[32–40]
Selection	6 papers—[41–46]	28 papers—[47–74]
Programming		

As a result of the literature review, we found 43 articles between 2007 and 2022. Of these, 37 articles (86%) correspond to qualitative proposals, where 9 articles (21%) are at the prioritization level and 28 (65%) at the control selection level. In addition, only 6 articles

(14%) propose quantitative methods for selecting security controls. These results indicate that the vast majority of the proposals are concerned with the problem of security control selection, but only a few resort to quantitative methods from Operations Research to solve them. However, these proposals do not define a methodical process that completely covers the definition of the best set of controls to recommend but rather propose quantitative techniques to be used at some point in the process. It is then up to the expert's judgment as to how to apply the methods recommended by each proposal.

On the other hand, from the literature review, it is evident that there are no proposals that address the problem of scheduling the implementation of the selected controls, unlike our proposal, which defines a set of methods to support this process.

Figure 2 shows the distribution, over the years, of the articles found.

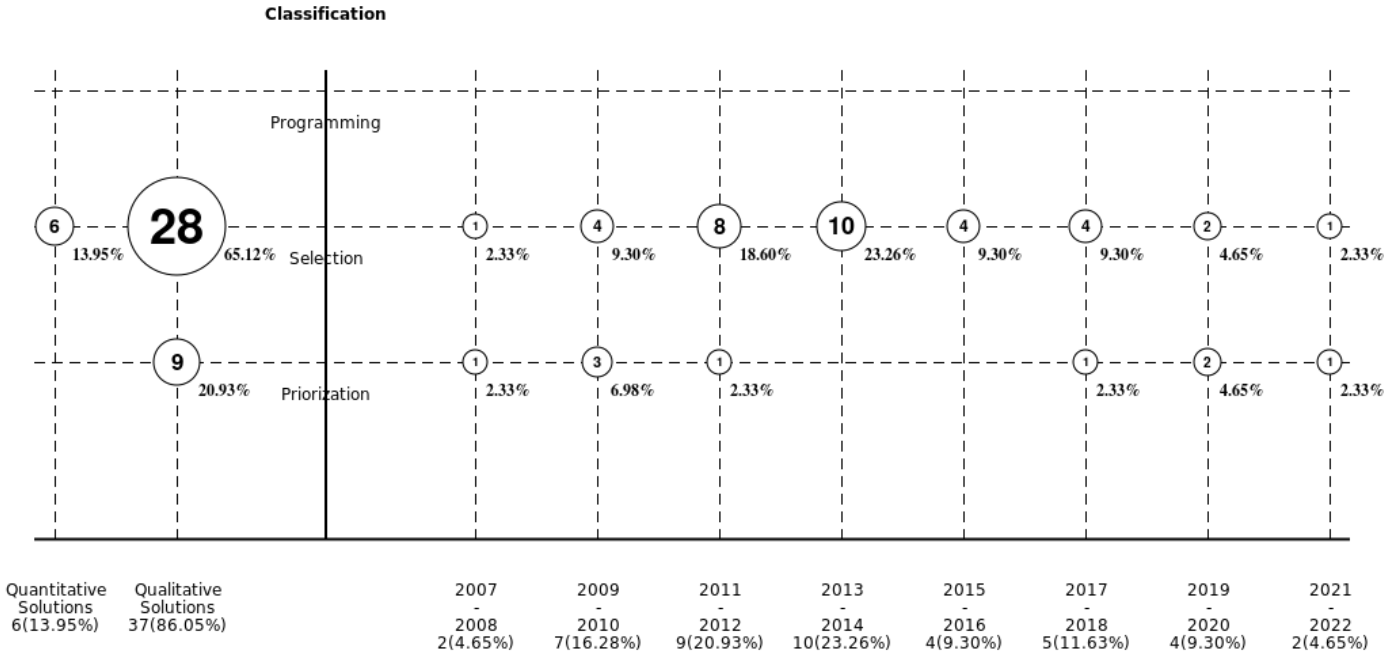


Figure 2. Bubble diagram of Systematic Mapping results.

In this image, we observe that the most significant number of articles is concentrated between 2011 and 2018, with 26 (60.4%) proposals focused on the "selection" level. We also note that, although the number of articles has decreased in the recent years, proposals continue to be developed, so we consider it a problem of interest to the community.

From the above, we conclude that the recommendation of improvement actions is a desirable stage in operation and evaluation of an ISMS. However, both the different standards that regulate the implementation and operation of the management system, as well as the practices identified in the industry, do not provide a methodological framework to support the process of identification and selection of improvements, leaving the application of the selection techniques to the expert's discretion.

3.2. Phase 2: Proposal Design

From the literature reviewed, it is possible to describe a general process for selecting security controls, which reflects the main steps to follow to make recommendations for implementation, supporting and directing the expert towards obtaining the optimal subset based on the particular characteristics and limitations of each organization.

As described in Figure 3, the main contribution of this proposal is the definition of a systematic process that, based on diagnostic information and the particular conditions of the organization, guides the generation of a model that represents the improvement intention based on the organization's constraints. This model is constructed as an optimization

problem since it seeks the best solution to the progress problem defined by the organization. Thus, the model will be solved by the optimization technique that best suits the situation. The resolution of this model will provide the best set of security controls that adhere to the constraints imposed by the organization.

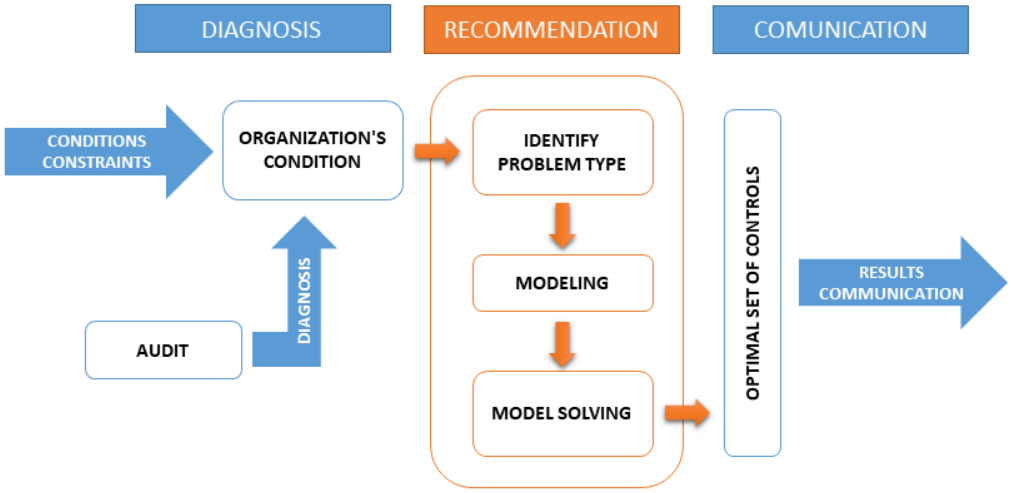


Figure 3. MASISCo Stages.

Given that the aim is to optimize the selection of controls based on a set of objectives and conditions that may vary from one organization to another, the proposal defines the following processes: processes dedicated to gathering the organization's needs (diagnostic stage), processes to recognize the problem, model the situation and resolve the optimization model (recommendation stage), and finally, the definition of processes and formats to disseminate the results of the study (communication stage).

3.2.1. Diagnostic

This stage considers the process that allows obtaining the information that reflects the current state of the ISMS performance. This diagnosis evidences the weaknesses of the system and determines which is the gap that the organization must cover to improve the performance of its ISMS. The previously reviewed standards consider this stage, ISO/IEC 19011:2018 and ISO/IEC 27001:2013, provide a clear methodological framework regarding the actions to be carried out to collect the diagnostic information.

As a way of supporting the diagnostic process and obtaining information, the proposal includes a questionnaire that allows the security assessor to collect information on the organization's current status concerning compliance with the information security standard. This questionnaire was created based on the criteria and indications of the ISO/IEC 27001:2013 standard. In addition, the questionnaire allows the entry of relevant parameters for modeling the situation, such as costs, times, and benefits.

3.2.2. Recommendation

From the diagnosis results, it is possible to know the gap that the company must cover if it wants to reach a certain level of risk or a degree of conformity with the standard. For this, it is necessary to define an improvement plan, which determines the set of controls or security criteria necessary to achieve the risk or compliance goal, considering the characteristics and resources of the organization. Despite this need, there is no methodological framework based on quantitative optimization techniques to support this process. This situation leads to subjectivity in recommending an improvement plan since much of the process is subject to the analyst's experience.

Accordingly, a large part of this proposal is framed by defining a methodical and replicable process that defines the procedures, techniques, and tools that support the

definition of a plan for the implementation of security criteria or controls within a given time frame and according to the goals, strategies, and resource conditions of each organization.

Then, in the Recommendation stage of this proposal, we seek to solve the subjectivity problem by incorporating optimization methods and techniques for modeling and solving the scenarios that represent the problem of the selection of security controls.

As shown in Figure 4, we have divided this stage into three major processes:

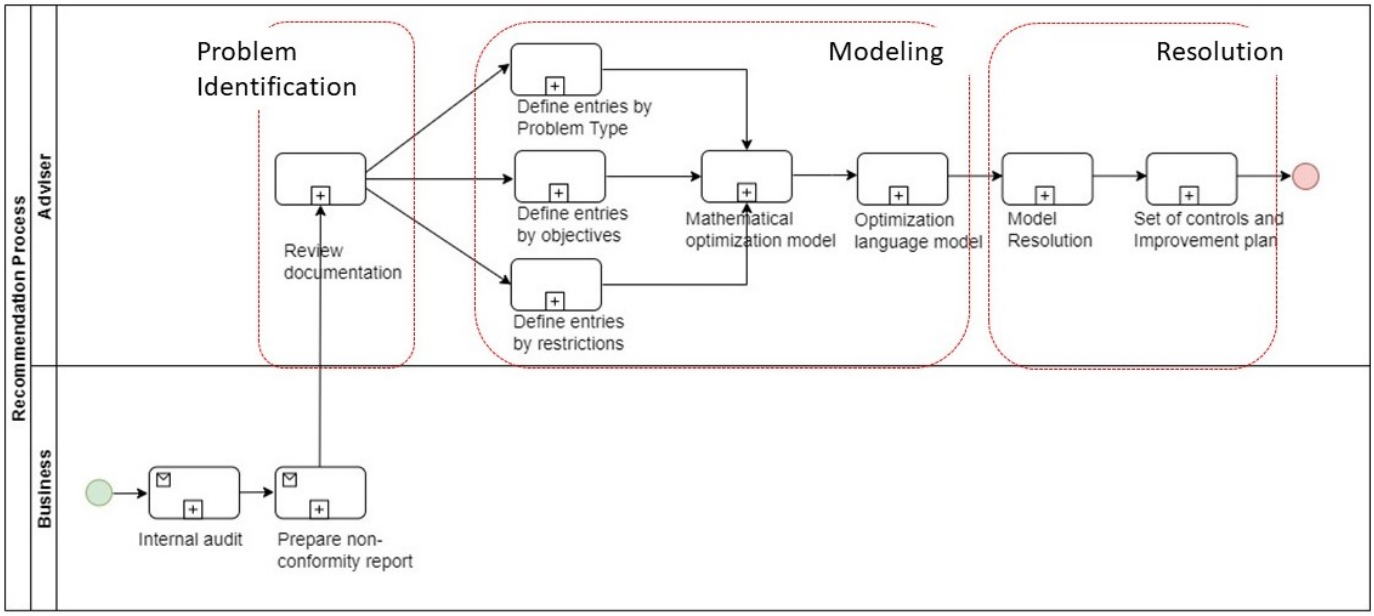


Figure 4. Detail of MASISCo stages.

a The first refers to the identification of the optimization problem to be solved. The result of this stage is a detailed description of the problem, which specifies: (i) the objective, (ii) the constraints to be considered, and (iii) the parameters of the variables that define the objective, as well as the organization's constraints.
Table 2 summarizes seven situations a security assessor may face when making recommendations. We have classified them according to their objective, in order of increasing complexity: prioritization, selection, or scheduling problems.
The prioritization of controls refers to ordering controls concerning one or more criteria, for example, risk or cost, prioritizing from highest to lowest value or vice versa.
In the case of selection, there is a recommendation of a subset of controls concerning the entire set based on the organization's objectives and constraints.
In the case of scheduling, it not only selects a subset of controls but also determines the implementation sequence of the selected controls based on some criteria.
In addition, for each situation identified, we list the OR technique or method that can be applied for its modeling and solution.
These situations are detailed in depth in [31]. This definition of problem types, categorized by objective, facilitates subsequent modeling since each of these situations requires different modeling and the use of different OR techniques for their resolution. Thus, the proposal supports security advisors in selecting these modeling and resolution techniques for the situation.

Table 2. Summary of Types of problems and solution methods.

Category	Situation	OR Method	Priorization	Sequence	Selection	Programming	Function Objective	Nesting
Prioritization	Multidimensional ranking of controls	[75,76]	✓					
	Sequencing of independent controls	[77–79]		✓			Single	
Selection	Selection of controls with restrictions	[80–84]			✓		Single	
	Selection of controls with restrictions and dependencies between controls	[80–84]			✓		Single	✓
Programming	Dimension sequencing and control programming with nesting	[85,86]		✓	✓	✓	Single	✓
	Selection and programming of controls considering nesting	[82,87–90]			✓	✓	Single	✓
	Multi-criteria programming of constrained controls	[82,90,91]			✓	✓	Multi	✓

b The second process refers to modeling the situation as an optimization problem. The result of this stage is the mathematical model derived from the formats found in the OR field.
In this process, it is necessary to determine the conditions and restrictions to be included in the modeling. In this sense, the proposal proposes the need to establish three aspects:

- Improvement plan objectives;
- The constraints of the organization;
- The relevant parameters for modeling.

Concerning the objective sought by the organization, it must establish what it hopes to achieve or satisfy with the selection process. Some examples of valid objectives are:

- Maximize the number of controls to be implemented or maximize the benefit of implementing the group of controls;
- Minimize the risk of non-implementation of controls, or minimize the implementation time of the group of controls.

According to an optimization problem, these objectives represent the model equation that will drive the resolution of the problem. Therefore, it is important to clearly define what the organization is looking for when selecting the subset of controls. In addition, the situation to be modeled may have more than one objective, such as maximizing implementation progress and minimizing risks, which would correspond to a multi-objective problem and thus apply other optimization techniques.
On the other hand, it is also necessary to establish the conditions or restrictions the organization must consider when making the recommendation. Usually, these restrictions are associated with the availability of resources that the organization has to implement a possible improvement plan. Some examples of restrictions could be:

- A certain budget level;
- A specific time to carry out the implementation project;
- A certain level of risk that the organization needs to reduce.

Finally, in order to perform the modeling of the constraints and objectives, it is necessary to establish some relevant parameters for the modeling, such as:

- Implementation cost per control;
- Implementation time for each control;

- The benefit associated with the implementation of the control;
- Risk associated with each control.

Once the consultant has defined the parameters, the model equations and the variables that comprise them are constructed. To define these equations, it is necessary to determine which are the variables that, in the IS context, allow modeling the situation as an optimization problem. In [31], we proposed an ontology that integrates the main concepts and variables found in a selection problem. In Figure 5, we refer to this model.

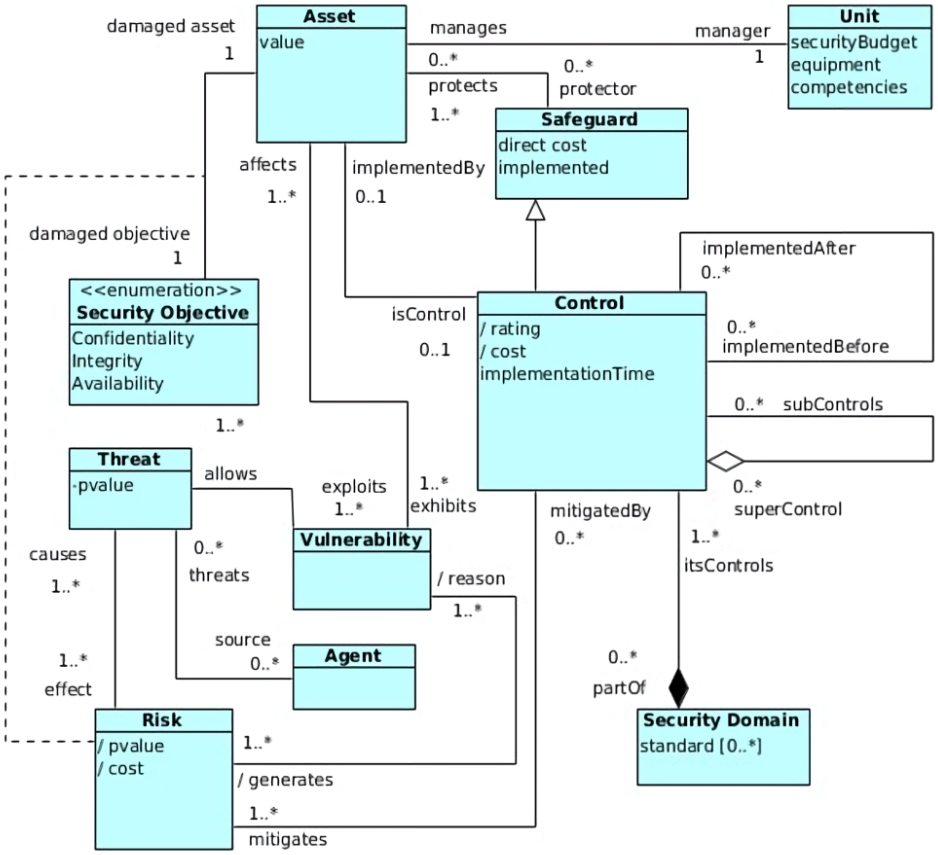


Figure 5. Information security conceptual model [31].

Generally speaking, any concepts in the diagram can be part of an objective function, and the different paths defined by their navigability are potential constraint considerations.

c Finally, the third process refers to the solution of the proposed model through the various optimization problem-solving techniques proposed in the OR.
The problem of model-solving is relatively simple. First, the model developed in the previous step is written in some modeling language for optimization problems. After this step, the resolution can be done manually, using the various techniques for solving this type of problem, or using some tool or computer application that supports these techniques.
Several software packages cover this process supporting different optimization languages. Some of these applications are summarized in Table 3. In addition, as can be seen, there are several free or paid options for Web environments or workstations that support different modeling languages for this type of problem.

Table 3. Overview of modeling languages for optimization problems.

Spreadsheets with associated Solver	
All mathematical formulations that can be solved through the properties of a spreadsheet program are considered. In general, they are applied to solve simple problems which do not require very complex modeling, such as linear programming problems.	Solver MsExcel
Mathematical and symbolic calculation environments	
Applications dedicated to solving mathematical problems that include their Solver. These programs can solve more complex optimization problems since they have functionalities dedicated to these types of problems.	MatLab Maple Mathematica NEOS-SERVER
Algebraic modeling languages	
This type of language and associated tools have specific capabilities for resolving this problem. The syntax allows building a model very close to the mathematical expression that represents the situation.	GAMS AMPL AIMMS XPRESS-MP

3.2.3. Communication

This stage considers the communication of recommendations regarding the selection of controls. According to the provisions of ISO/IEC 19011:2018, depending on the conditions of the audit, the final report may include, among other points, the following information:

- Opportunities for improvement, if specified in the audit plan;
- Agreed action plans, if any.

As seen from the standards reviewed, there is no standard format regarding the content and form for presenting the results of an audit since it is not stipulated as part of the final report unless previously agreed with the auditee. However, if an improvement plan is required, it is possible to define a format for the communication of these results that includes:

- Recommended controls;
- Value of the target achievement (objective function);
- Summary of resource utilization (constraints).

As seen in Table 4, our proposal covers weaknesses presented by other proposals found in the literature and information security standards. However, unlike the proposals reviewed, MASISCo defines optimization solutions for the three problem domains that we identified (Prioritization, Selection, and Programming), considers the dependencies between controls, and proposes the development of an ad hoc tool to support the process. On the other hand, MASISCo covers the deficiency of standards, defining a methodological approach that systematically addresses the problem of recommending security controls.

Table 4. Comparative table of proposals.

Items	MASISCo	Literature Proposals	Security Standards
Formalizes recommendation process	Yes	No	No
Incorporates optimization methods	Yes	some	No
Considers nesting controls	Yes	No	No
Proposes Software tool	Yes	No	No
Proposes solutions for:			
- Control prioritization	Yes	Some	No
- Control selection	Yes	Some	No
- Implementation Programming	Yes	No	No

3.3. Proposal Validation

In order to measure the performance of the proposal and the perceptions that security assessors would have about it, we conducted an empirical study on the adoption intention of this methodological framework. The study is based on the unified model of adoption of

methods in Software Engineering UMAM [28] and analyzes the adoption intention of the proposal in an academic context.

UMAM is a method adoption model that provides a framework for assessing the intention to use a working method by a group of professionals. Although this model was indeed developed with its application in mind for studies in the field of software development method adoption, its structure and theoretical foundation allow its application to any method that implies a change in how the IT professional works.

As shown in Figure 6, the model proposes that the intention to adopt a new method is explained based on five aspects or dimensions. To collect the information, the model proposes a measurement instrument in the form of a questionnaire called UMAM-Q, which supports the theoretical model.

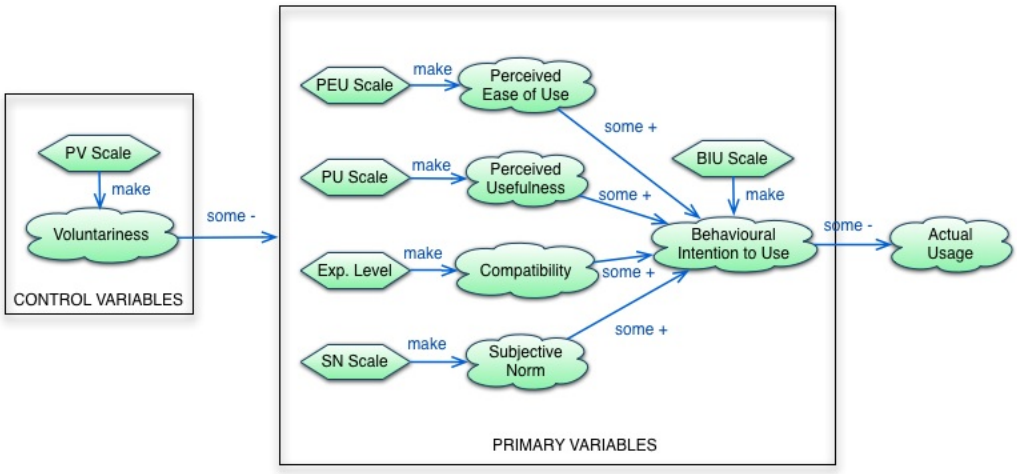


Figure 6. Unified Method Adoption Model (UMAM).

The study was conducted during the second semester of the year 2020, with a total of 12 students of Computer Engineering. Three stages were developed to apply the study: (i) training, (ii) application, and (iii) evaluation of the experience.

- Training: As a first stage of the experience, students needed to be trained in using the proposed methodological framework. Then, the students had to solve a set of hypothetical cases. Next, they had to identify a set of "non-conformities" and propose an improvement plan by selecting the optimal set of controls. Then, half of the hypothetical cases were to be solved traditionally, i.e., based on the study of the standards and their analysis of the situation, while the other half were to be solved using the proposed model. Finally, each student was randomly assigned a set of cases to solve.
  Given the impossibility of splitting the groups to control the possible effect or bias that the order of the treatments (without/with the help of the proposal) could have on the results, the students first carried out the case studies without using the proposal. After this stage, they were trained in using the proposal, through its application in various cases and examples. At the end of this phase, we can assume that the students had the same skill level with both treatments.
- Application: After applying the proposal in the training cases, the students carried out an audit project in an organization of their choice in the context of Information Security. In this project, the students formed teams of three people. Each group applied the proposal to subsequently evaluate the level of suitability of the proposal for the resolution of actual cases.
  The students were guided by the phases defined in ISO/IEC 19011:2018 [30] and by the controls proposed in ISO/IEC 27002:2013 [92]. In the diagnosis and improvement plan phases, the teams had to apply the process and models proposed in this work.

For modeling the optimization problem, they used the GAMS language [93] and built it from the data obtained from the audit. For the resolution of the resulting system, they used the web portal for solving optimization models, NEOS-Server [94].

- Evaluation:The final step of the study consisted of students evaluating, using the UMAM-Q instrument, the usefulness, ease of use, social norm, and perceived compatibility, as well as their intention to use the proposal in the future for diagnosis and making safety recommendations.
  For the analysis of the student's responses, we applied three types of studies: (i) analysis of descriptive statistics, (ii) analysis of qualitative responses, and (iii) multiple linear regression study.

Result Analysis

We have not considered the dimension of "Voluntariness" in the analysis since the academic context in which the students carried out the project forced them to use the method, so this domain loses meaning for the analysis.

First, we analyzed the descriptive statistics related to the dimensions of the UMAM model. In addition, we conducted a qualitative analysis of the main advantages and disadvantages of the proposal through the answers to the open-ended questions of the questionnaire. The students indicated the advantages and difficulties they perceived in applying the proposal. Finally, a quantitative analysis is presented, through a multiple linear regression model, applied to the student's answers.

Descriptive Statistics

For the characterization of the dimensions of the UMAM model through descriptive statistics, the SPSS statistical analysis tool was used. According to the structure of the instrument, the Utility (U), Ease of Use (EU), Compatibility (C), and Subjective Norm (NS) dimensions present a scale of 14 items, each with scores from 1 to 7, where 1 is the worst perception (Strongly Disagree) and 7 the best perception (Strongly Agree). Therefore, the score range for these variables goes from 14 points to 98 points. On the other hand, the Behavioral Intention (BI) dimension presents a 7-item scale, with a score range from 7 points to 49 points.

Table 5 summarizes the descriptive data for each dimension, while Figure 7 presents box plots for each model's dimensions.

Given the data presented in Table 5 and in the graphs in Figure 7, the high perceived usefulness of the proposed method stands out. This dimension presents a median of 78.5 points out of 98. This value implies that the students perceive the method as helpful when solving the problem.

The dimension Compatibility also shows a high median, 71.5 points out of a maximum of 98. This value indicates that the students perceive the method to be compatible with the work style that a future specialist expects to perform.

At the other extreme is the dimension Subjective Norm , whose median is 57.5 points out of 98. This value is explained by the fact that students know that this method is not the industry standard and do not feel any external pressure to use it. Given that there is no industry-standard alternative, we hypothesize that this dimension does not necessarily have a significant impact on the student's decision to adopt this methodological framework.

In addition, the analysis reflects that the main weakness of the proposal is the Ease of Use dimension since it presents a median of 60.98 points out of a maximum of 98, which is significantly lower than the Usefulness and Compatibility dimensions. Initially, it seems that students perceive the method as challenging to assimilate and not very intuitive. Therefore, this dimension is the priority area of improvement for future iterations of the proposal.

Finally, about the **Intention to Adopt**, the median is 35 points out of a maximum of 49, which implies a slightly positive intention toward adoption.

Table 5. Descriptives of UMAM dimensions.

Usefulness	Mean		77. 8
	95% Confidence interval for the mean	Lower limit	69.31
		Upper limit	84.86
	Median		78.50
	Minimum		56
	Maximum		94
Ease of use	Mean		65.42
	95% Confidence interval for the mean	Lower limit	56.49
		Upper limit	74.45
	Median		60.50
	Minimum		47
	Maximum		91
Compatibility	Mean		68.92
	95% Confidence interval for the mean	Lower limit	57.02
		Upper limit	80.81
	Median		71.50
	Minimum		34
	Maximum		91
Subjective Norm	Mean		58.67
	95% Confidence interval for the mean	Lower limit	50.15
		Upper limit	67.18
	Median		57.50
	Minimum		35
	Maximum		83
Intention to Adopt	Mean		34.67
	95% Confidence interval for the mean	Lower limit	29.05
		Upper limit	40.28
	Median		35.00
	Minimum		17
	Maximum		49

Qualitative Opinions

In order to obtain qualitative information on the subjects' perceptions, the evaluation instrument included a section of open-ended questions, where the student could state three positive and three negative aspects related to the implementation of the proposal. The analysis of these opinions made it possible to understand better the student's perception of the benefits and difficulties of the proposal and to give or take away reason from the initial intuitions obtained through the descriptive statistics.

To facilitate the analysis of student opinions, we categorized student responses concerning the components of the UMAM model, so we assigned each response to one of these components: U—Usefulness, EU—Ease of Use, C—Compatibility, and NS—Subjective Norm.

Table 6 shows the percentage of positive comments associated with each UMAM dimension: 47.6% refer to aspects of U, 38.1% to aspects related to C, and only 14.3% to aspects related to FU.

Table 6. Summary answers—Positive aspects.

Dimension	Answers	Percentages
U	10	47.6%
EU	3	14.3%
C	8	38.1%
NS	0	0%

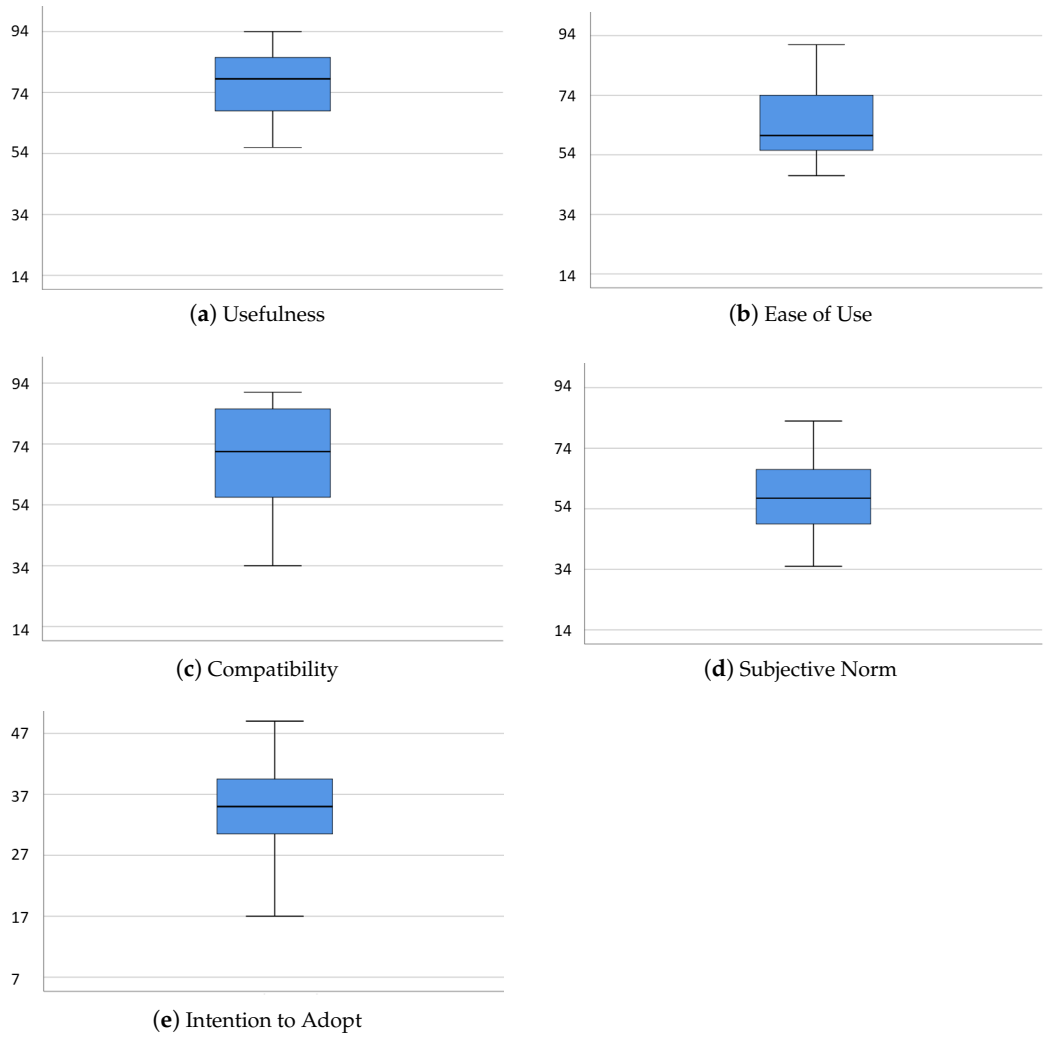


Figure 7. Descriptive Statistical Graphs.

These values indicate that the students perceive that the main strength of the proposal is that it contributes to greater effectiveness and efficiency in the work of the security consultant (U). In addition, they highlight its generality and structuring qualities (C). On the other hand, only 14% of the comments indicate that the proposal is not complex to learn and use (FU). Finally, the NS dimension is not mentioned in any of the comments.

Table 7 summarizes the percentage of negative responses related to each model dimension. Of these opposing opinions, only 18.75% refer to U and only 6.25% to C. However, 75% of the comments point directly to FU as the main problem with the proposal. Again, NS does not appear in the comments, adding weight to the initial hypothesis that, being a methodological framework dealing with a problem for which there are no standardized alternatives, it is not an aspect to which the subjects give greater importance concerning the other domains.

Table 7. Summary answers—Negative aspects.

Dimension	Answers	Percentages
U	3	18.75%
EU	12	75%
C	1	6.25%
NS	0	0%

These percentages show that students perceive the proposal as challenging to use and learn, that it requires previous knowledge, and that if they do not have it, it takes a considerable time to obtain it. To a lesser extent, they think they need to model the problem may slow down their work under certain conditions. Finally, one opinion refers to the fact that this is not the usual way they are used to programming, which causes them some difficulties related to C.

Faced with these results, we hypothesize that the high percentage of negative responses in the Ease of Use domain is mainly due to the inadequate training of Computer Science students regarding OR, especially in modeling and solving optimization problems, which hinders the use of the proposal.

As can be observed, the qualitative opinions of the students are consistent with the scores obtained through the UMAM-Q instrument. Therefore, we conclude that the proposed methodological framework is a helpful tool to support the decision-making process in selecting controls for a proposed improvement in the progress of compliance with a standard. Furthermore, it is an instrument compatible with the assessor's practices. However, it is not easy to use since it requires previous knowledge in modeling optimization problems and presents a marked learning curve.

This last point is the major weakness of the proposal. It implies that a security assessor must acquire knowledge in OR techniques for modeling and solving optimization problems if the latter wishes to benefit from the advantages of using the proposal. This weakness makes the development of techniques, artifacts, and tools to facilitate modeling and problem-solving the foremost opportunity for improvement of the proposal.

Quantitative Analysis: Multiple Linear Regression

Finally, we performed a pilot multiple linear regression analysis to recognize the impact of each independent variable (U, EU, C, NS) on the dependent variable (IoA). This analysis aims to quantify the degree to which the independent variables explain the dependent variable.

It is important to note that, given the small number of observations, the conclusions of this analysis should be treated with great caution. Our goal in doing so has been not to create a predictive model but rather to add or de-emphasize initial intuitions about the relative weight of the independent variables analyzed to adopt this method. This information is essential for planning how to prioritize future improvements to the method.

To ensure the applicability of the study, we had to validate the following conditions:

a. The dependent variable is of the ratio type (continuous).
b. The independent variables are ratio type.
c. There is a linear relationship between the dependent and independent variables, individually and collectively.
d. Homoscedasticity of variances.
e. Independence of observations.
f. There is no multicollinearity between the independent variables.
g. No hay puntos inusuales o que influyan de manera indebida.
h. Residuals of the regression line follow an approximately normal distribution.

The results of the multiple regression analysis show how all variables are relevant for calculating the CI. As shown in Figure 8, the multiple correlation coefficient shows an R-value of 0.869 (strong), with an adjusted coefficient of determination of 0.663, i.e., the model explains 66.3% of the variability in IoA, which, according to Cohen, is a large effect size.

Model	R	R-Squared	Adjusted R-squared	Standard error	Durbin-Watson
1	0.869	0.755	0.663	5.132	2.227

Predictors: (Constant), Usefulness, Ease of Use, Compatibility
Dependent variable: *Adoption intention*

Figure 8. Multiple linear regression model summary.

Therefore, according to the information presented in Figure 9, the regression model results in Equation (1):

$$IoA = 7.914 - 0.105 * U + 0.1 * EU + 0.411 * C \quad (1)$$

MODEL	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Deviation	Beta		
1 (Constant)	7.914	10.326		0.766	0.465
Usefulness	- 0.105	0.201	- 0.145	- 0.521	0.617
Ease of Use	0.1	0.148	0.158	0.675	0.519
Compatibility	0.411	0.128	0.87	3.206	0.013

Figure 9. Regression model coefficients.

On the other hand, given the small number of observations, we see that the confidence intervals for all the variables are extensive. These data imply that C is the only variable whose impact on the IoA is positive (we can be 95% sure that C will always have a positive impact on the IoA). Moreover, C is the only statistically significant coefficient, implying that C has a linear relationship with IoA.

From the above, we can conclude that to boost the adoption of the proposed method among computer science students, we need to ensure that they perceive it as a method that is highly compatible with how they believe it should work. This perception impacts their IoA more than others traditionally considered more important, such as perceived U and EU.

As conclusions of this study, we can mention the following:

a Students reacted favorably to the proposal.
The evaluation results show that they are consistent among the three types of analysis performed. These results indicate that the students perceive the methodological proposal as a helpful tool for selecting the set of security controls that best fits the conditions of the organization under study. In addition, the students perceive that the proposal is compatible with how the security professional works, which indicates that it is in line with the work of a security assessor, so it can be considered a contribution and not a hindrance for the assessor. On the other hand, the students perceive that the proposal presents a certain degree of difficulty in its application, mainly due to the student's lack of knowledge of OR techniques to solve an optimization problem.
Regarding the IoA of the methodological proposal, it presents a slightly positive trend, which implies that there is a good chance that the subjects will adopt the proposal. However, this possibility is not high, so there is room for improvement. In addition, if we consider that the students expressed as weakness the FU and that the IoA is strongly related to the perception of the C of the method, we can deduce that improvement actions should focus on these two aspects preferentially.

b The proposed model is consistent.
Analysis of the three studies' results shows the proposal's consistency concerning the factors that explain the IoA. This effect is evidenced in the student's responses, collected with the UMAM-Q instrument, the qualitative perceptions stated by the students, and the Linear Regression study applied to reflect that the strengths of the proposal are C and U. At the same time, the main weakness lies in its EU.

In addition, from the results of the regression study, it was also evident that the model is highly significant, which implies that the UMAM is a reliable model for predicting IoA. The above, together with the results of the qualitative study and the analysis of the descriptive statistics, give great significance to the opinions of the students, so we can be confident in the results that indicate that the methodological proposal is an excellent tool to support the decision-making process regarding the selection of security controls.

On the other hand, given the characteristics of the experience, we can highlight the following as situations that threaten the validity of the study:

a Size of the study group.
The main problem with the study is the low number of subjects who took part in it. Only 12 students responded to the consultation instrument. While it is true that this number represents 100% of the universe of students involved in the study, the group is insufficient, so it is not possible to generalize the results to the general population of auditors, not even audit students. However, these results make it possible to establish a trend and basis on which to design a future process of improvement to the proposal before expanding it to other areas and carrying out a more ambitious empirical study.

b Study group characteristics.
Another important factor to consider, also related to the study's external validity, is the group's representativeness with respect to the target audience of the proposal. We recognize that the students included in the sample are not expert security advisors but have basic knowledge of the area and the practices of a security advisor. However, it is worth mentioning that the subject within the study program aims precisely to provide this knowledge to the student and that it is the only subject dedicated to this area so that any recent graduate will have the same knowledge as the students who participated in the study. In addition, we train students in applying the methodological approach, constructing and executing the optimization models, and interpreting the results.

3.4. Support Tool

To facilitate the implementation of the proposed process, we have developed a software tool to assist the expert in determining the best set of controls to solve the problem. As shown in Figure 10, this tool automates much of the proposal, providing software support for data collection, automatic generation of the optimization model, and automatic resolution of this model, which allows obtaining the optimal set of controls that satisfies the conditions of the problem.

As shown in Figure 11, we designed the tool's architecture so that it continues to be enriched through the permanent inclusion of new cases or types of problems since, given a large number of variables and possible scenarios in the formulation of the model, there is a large number of cases or examples that can be produced and that we have not included in this first development.

The tool comprises two main modules. The first is related to the collection and management of the organization's baseline information, i.e., the diagnostic information that shows the organization's compliance status and serves as a baseline for the improvement plan proposal. In this module are the components related to the survey that allows the collection of information, the costs and implementation times, and the risk associated with each control. It also defines the storage of this information for subsequent modeling.

On the other hand, the second module is related to the development of the optimization model based on the base information of the organization. In this module, we develop the components that allow us to define the type of optimization problem associated, the OR resolution techniques to be used, and the generation of the model in GAMS. This module also includes the components that allow us to communicate our tool with the NEOS-Server web system, to send the model and the data for its resolution.

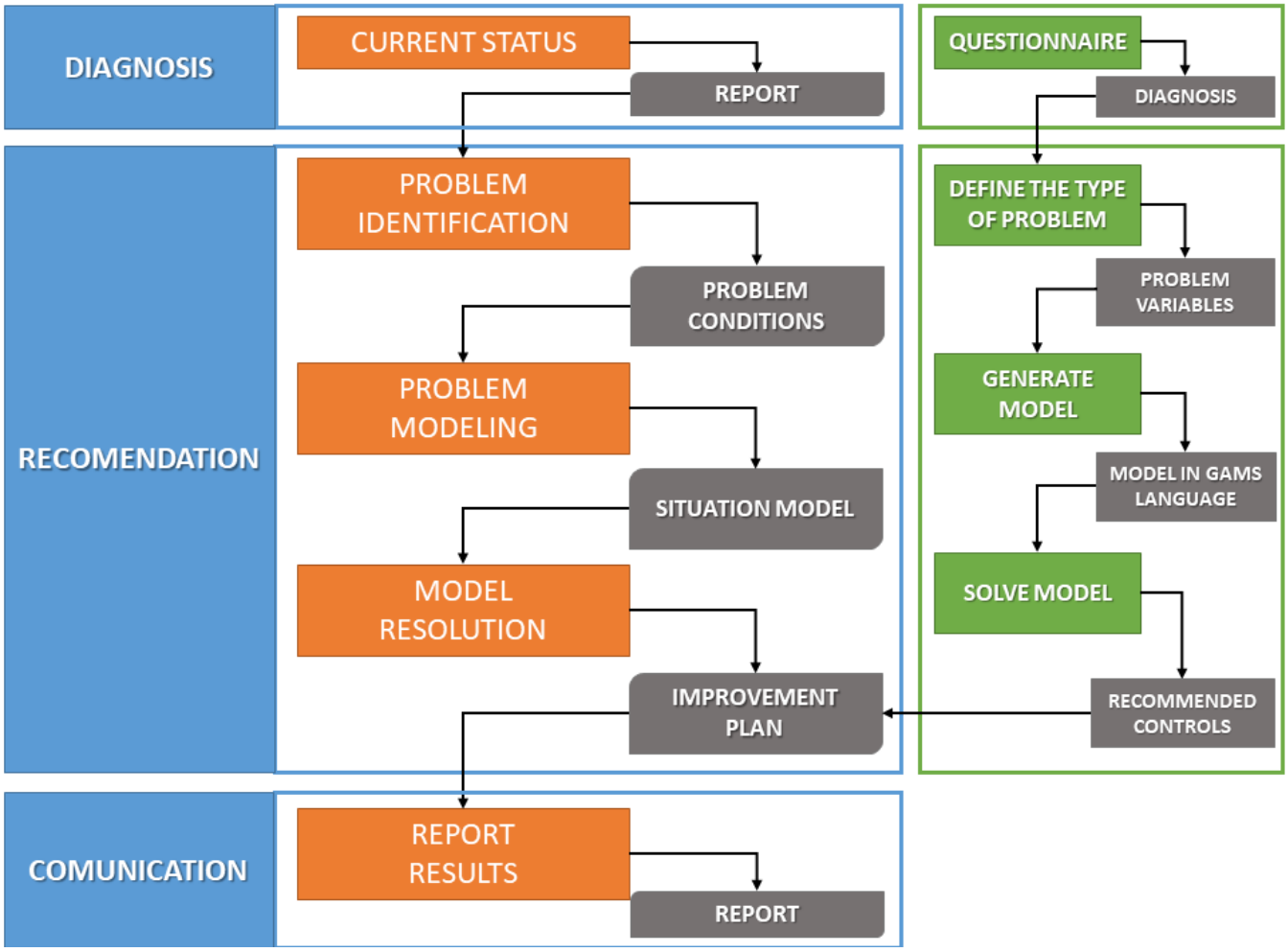


Figure 10. Process stages covered by the tool.

In Figure 12, we present some images of the tool at different process stages.

The tool supports practically all the phases proposed in the methodological approach. Thus, in each of the phases, the tool is present and allows for automating most of the processes involved.

In the diagnosis, the tool supports the process of capturing and visualizing information. Through a questionnaire built from the ISO27001 controls, the user can describe the organization's status concerning the standard. With these answers, it is possible to determine the degree of conformity of the organization concerning the standard, achieving a preliminary diagnosis of the organization. In addition, the system allows entering the cost of implementing the controls, the benefits associated with their implementation, risks, and implementation time, depending on the type of problem to be modeled.

The answers and settings provided by the user are stored in the system for the subsequent optimization model development. The tool can design an optimization model in the recommendation stage, from the negative answers, the problem type configuration, and the variables involved.

In the recommendation stage, the tool automates the generation of the model in the GAMS language and its resolution through the NEOS-Server web platform [94]. The first phase of this step refers to the definition of the type of problem to be considered and the variables involved in the modeling (objective function and constraints). For the completion of this step, it is sufficient for the user/advisor to have selected the type of problem to be solved. The tool allows (i) defining the type of problem, (ii) configuring the type of Solver to be used, (iii) defining the available budget, and (iv) defining the type of optimization to be performed (maximize or minimize).

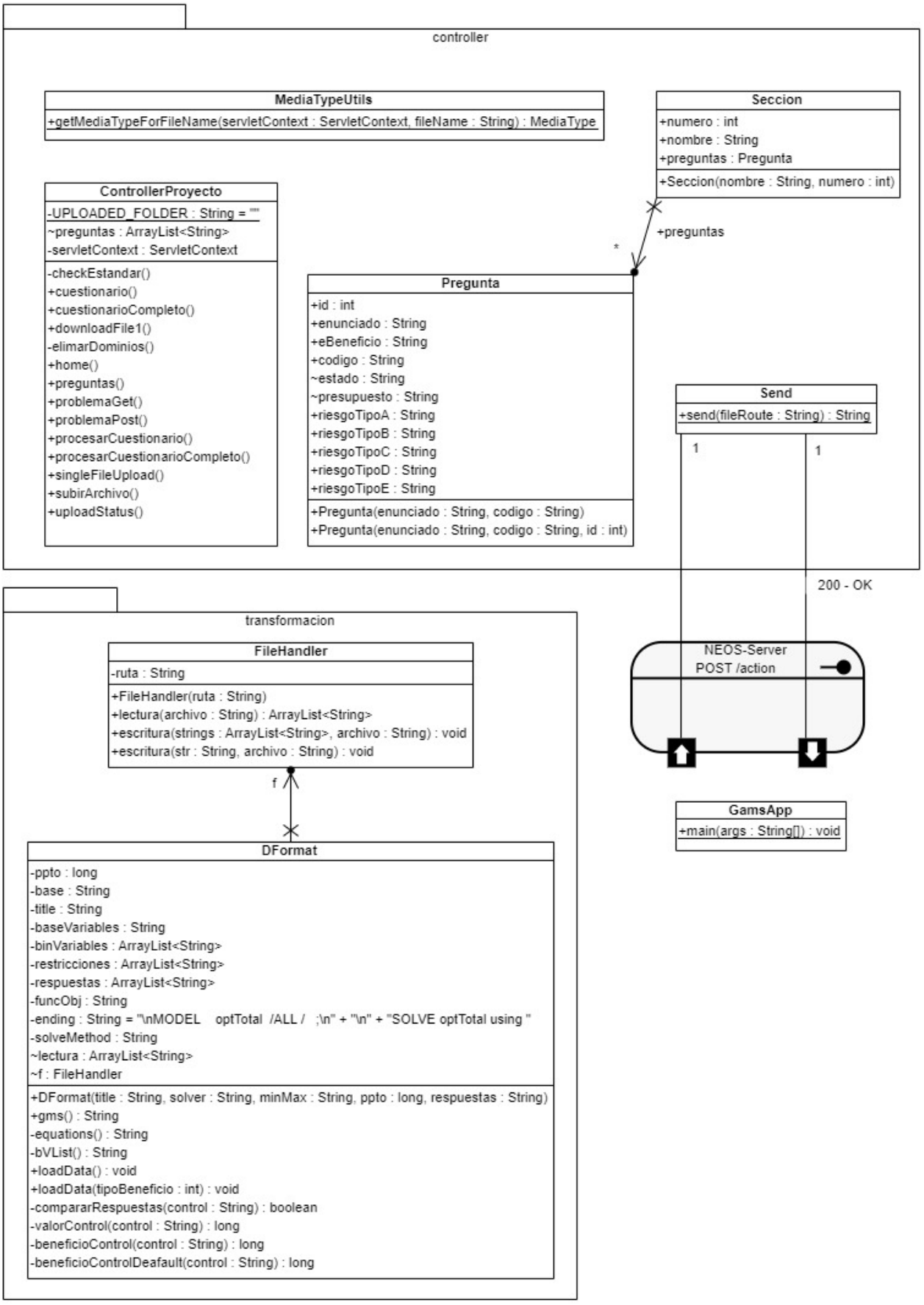
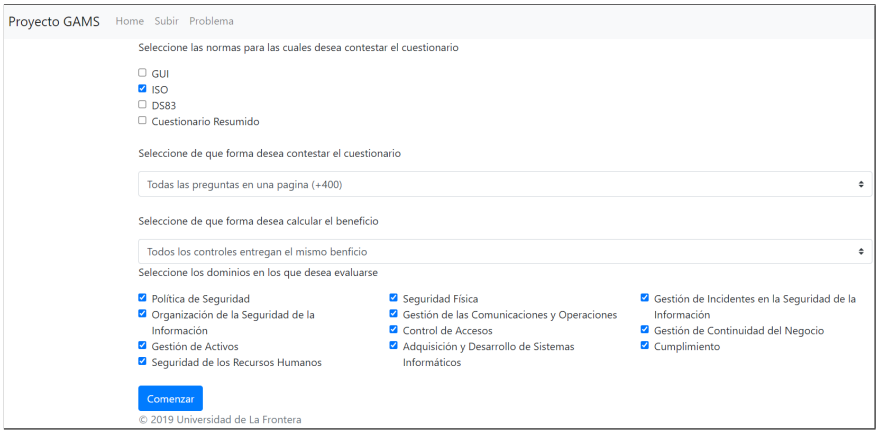


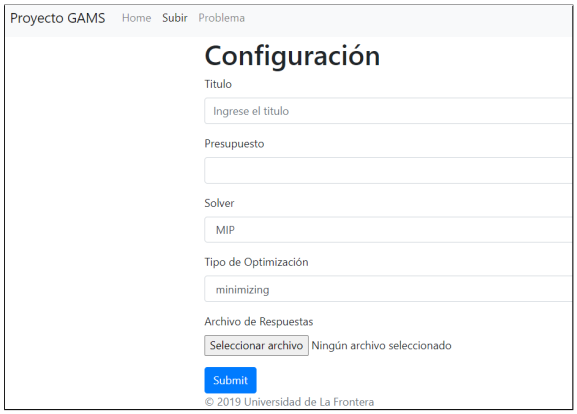
Figure 11. Tool architecture.

With the model built, the application uses the free optimization problem-solving engines proposed by NEOS-Server. Finally, the tool uploads the file to the web portal and receives the response file. These responses are displayed by the tool and constitute the control selection proposal.



(**a**) Problem configuration

(**b**) Questionnaire



(**c**) Solver configuration

Figure 12. Support tool images.

We note that the tool developed is a first prototype that, although functional and complete for a subset of the cases described in this proposal, suffers from several shortcomings:

- It does not cover all possible casuistry of optimization problems.
- Currently, the tool does not display reports or interpretations regarding the selected set of controls but only delivers the file provided by NEOS-Server for manual reading.

This emerges as opportunities for improvement and/or future work in regard to tool development:

- Continue including the optimization cases described in the proposals, with their respective variants.
- Improve the way results are displayed and develop new views for viewing and interpreting reports with the optimization process results.
- Validate the use of the tool through an empirical study showing its impact on the consultant's work.

However, beyond future work, the tool is a first step in improving the primary deficiencies of the methodological approach, which are mainly related to the difficulty of modeling and solving the optimization problem. Furthermore, this tool automates this part of the methodological approach to be "transparent" for the user.

4. Conclusions

Information Security has become very important in the work of organizations, given that in the recent years, there have been reports of severe breaches that several organizations have suffered in their systems, which meant losses of hundreds of millions of dollars to the world economy. Little by little, the awareness of the latent danger of not considering minimum security has grown worldwide. The multiplicity of types of attacks forces organizations to take a set of actions to eliminate any vulnerability or minimize the attack's impact. The actions proposed by a standard are transversal to the organization, affecting its organizational structure, policies, technological infrastructure, human resources, and processes, among other areas. This broad spectrum of application and resource limitations complicate the decision on how to implement security actions. The decision regarding the progress in achieving the standard is not trivial since it must consider various aspects of the organization, such as risk, costs, implementation times, prioritizations, and policies.

Security experts make progress recommendations based on their experience in implementing an ISMS. However, this approach is subjective and does not ensure an optimal recommendation since it does not follow a standardized process with well-defined steps and proven support techniques. Therefore, although this type of recommendation may meet the requirements and characteristics of the organizations, it does not optimize the use of resources.

The review of the existing literature showed that a high percentage of research (65%) focuses on proposing control selection methods based on qualitative techniques that do not ensure optimal solutions. In contrast, only 14% of the proposals define quantitative optimization models. However, these proposals also do not formalize a standard process or methodology for their application. In addition, it was also detected that there are no proposals to cover the scheduling of the implementation of the selected controls.

On the other hand, the review of some standards showed that they do not propose a formal or standard method for recommending an improvement plan (selection and programming of controls), so this stage relies on the opinion of experts, making it a subjective process.

In this context, this article proposes the design of a methodological approach for the selection and scheduling of controls of a security standard, using quantitative optimization techniques to support the decision-making of a security consultant.

A methodological approach such as the one proposed in this article is excellent support in decision-making since it defines a systematic and repeatable process supported by

mathematical techniques for modeling and resolving multi-objective problems, decreasing the decision time and increasing the accuracy of the recommendation.

One of the most relevant aspects of the proposed methodological approach is related to the identification and classification of the problems or scenarios that, on the one hand, characterize each organization and, on the other hand, define the situation towards which it wishes to advance. In this sense, this proposal identifies a set of 7 possible scenarios in which the problem the organization wishes to solve to achieve the safety standard can be categorized. Based on this classification, we propose optimization techniques that cover the solution to each scenario. The definition of the relationship between the problem and the applicable solution technique is configured as the core or the basis of the proposal for selecting security controls using the techniques of Operational Research. Therefore, it allows for simplifying the auditor's work significantly.

Then, the proposal not only categorizes the different scenarios that organizations can consider, from the most straightforward selection situations to schedule, but also associates the scenarios with the different optimization techniques for modeling and solving them, thus simplifying the analyst's work. Furthermore, modern optimization solutions have been demonstrated to address and solve security management situations from the OR perspective. Consequently, it is possible to argue that information security management not only has an excellent opportunity to improve its approach by incorporating the OR perspective but that OR also has, in information security management, an interesting domain to study.

The evaluation of the proposal made it possible to demonstrate, in an academic context, its impact on a security consultant. Furthermore, a method adoption study determined that there is a positive inclination towards using this methodological approach as opposed to the traditional solution.

Generally, the experience results for each dimension studied tend towards the positive ends of the scale. The descriptive statistics analysis for each dimension shows that the study subjects perceive the approach as a helpful process compatible with their way of working. Moreover, they show their predisposition to adopt the approach in the future if they can do so.

On the other hand, the main weakness of the proposal lies in the complexity of modeling the scenarios that represent the situation the organization wants to solve. Moreover, the modeling is done in an optimization language that is generally not in the domain of knowledge of a security consultant.

The results obtained in the analysis of the linear regression model, the analysis of descriptive statistics, and the qualitative analysis are consistent and point in the same direction regarding essential aspects for the subjects and opportunities for improvement. However, it is necessary to recognize some limitations of the study conducted. The most important is undoubtedly the size of the group and its characteristics, which means that the conclusions must be interpreted carefully.

However, it should be noted that the evaluation carried out was formative and, therefore, its purpose is not to study a finished product but rather, being the first application of the model, to determine a set of perceptions that will provide a series of opportunities for improvement.

Based on the conclusions of the method adoption study, we identified the need to support the user in the application of the methodological approach. For this purpose, we developed a prototype software tool that covers all the stages of the methodological approach, which provides even more excellent support to the security consultant in applying the approach.

This automation allows the expert to abstract from the complexity of modeling and solving the problem and focus his effort on analyzing the response, where the recommendation of the optimal set of controls is made explicit. In this way, the tool facilitates the consultant's task and the methodological approach's application. Moreover, in this way, it

is expected to account for the observations made about the proposal's ease of use, reducing the process's complexity.

Although we have not evaluated the tool's impact on the assessor's implementation of the proposal experimentally, it is possible to estimate that the use of the tool will improve the ease-of-use index of the model. Consequently, we expect that the automation of these processes of the proposed methodological approach will increase the adoption intention of security assessors.

A proposal such as this would have a positive impact on the recommendations for the implementation of an improvement plan based on the selection and programming of security controls since: (i) it formalizes a process that is currently not standard and depends mainly on the experience of the security consultant, (ii) by using optimization methods, it ensures optimal solutions according to the profile and restrictions of each organization, which optimizes time and resources, and (iii) by using software support, it automates a large part of the process, facilitating its application, reducing time and costs.

Therefore, the application of this methodology directly impacts the effectiveness and efficiency in the definition and implementation of the improvement plan to advance in the achievement of the safety standard. As a result, we perceive a positive impact on the maximization of resources, reduce the time considerably in the definition of the improvement plan and the costs, and ensure the determination of the best option based on the conditions defined by the consultant.

Finally, while it is true that the proposal presented in this paper has been fully defined, mainly in its conceptual framework, it is no less accurate that, from a practical point of view, work must continue to complete a 100% applicable process. Then, we propose the following points as the main lines of future research:

- The proposal includes a set of situations describing the possible scenarios an organization would like to advance. However, we recognize that this set is not definitive but can be completed by identifying new scenarios that organizations would like to incorporate into the model.
  Therefore, one way forward is to identify, in conjunction with security experts, other approaches to those already proposed, which will allow both to identify new ways to complete and improve those presented in this work and to identify additional cases to the types already recognized. With this information, a new consultation of the literature can be made to identify those optimization techniques or models that would allow the solution of the new scenarios proposed.
  In addition to the scenarios, we will include new information security standards or norms. This way, the approach will be able to cover better particular cases where the assessment must be based on one or more standards. Currently, the approach considers the ISO 27001 standard, the Supreme Decree 83 [95], and the Methodological Guide for information security of the Chilean Government [96].
- Another research path is related to the conceptualization of the information security field in identifying the variables that interact with this problem and the relationships between them.
  In this research work, we defined a conceptual framework that integrates a set of views of the problem. However, it is possible to expand it to consider new variables or relationships that were not identified. The same techniques can be used for this identification as the previous point, such as interviews or focus groups with security experts.
- The third line of work focuses on the future software tool development that supports the proposal. For example, if optimization problems and solutions continue to be defined, it is necessary to update the tool to incorporate these new scenarios. On the other hand, we must also update the tool concerning the new version of the ISO/IEC 27001:2022 standard and the controls present in ISO/IEC 27002:2022.
  This future development can be considered from the perspective of intelligent systems in such a way that the recommender becomes an assistant to the security expert, capable of supporting him in making decisions and guiding the creation and resolution

of scenarios that have not been considered from the beginning. In other words, the system could assist the user in creating models that represent the organization's reality, even if those cases are not considered based on the application.

- Finally, we must mention the need for future validation of the proposal with security experts in a professional context. The validation presented in this article, given that it was the first application of the proposal, was only aimed at identifying a series of opportunities for improvement through the collection of user perceptions. Nevertheless, with the conclusions from this study, it was possible to identify the proposal's weaknesses and implement the corresponding improvements.

Author Contributions: M.D. contributed to the development of the methodology approach, application and analysis of the study, development of the software tool, and writing the paper. C.C. (Carlos Cares) contributed to the conceptualization of the model, development of the methodology approach, and writing of the paper. C.C. (Cristina Cachero) contributed to developing the methodology approach, the study's application and analysis, and the paper's writing. Finally, J.H. contributed to evaluating the software tool and writing the paper. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Universidad de La Frontera, research direction, research project DIUFRO DI22-0043.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors acknowledge the technical support provided by Cristóbal Marinkovic.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Miloslavskaya, N.; Tolstoy, A. Internet of things: information security challenges and solutions. *Clust. Comput.* **2019**, *22*, 103–119. [CrossRef]
2. Mariano Díaz, R. *La Ciberseguridad en Tiempos del COVID-19 y el Tránsito Hacia una Ciberinmunidad*; CEPAL: Santiago, Chile, 2020.
3. Conteh, N.Y.; Schmick, P.J. Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks. *Int. J. Adv. Comput. Res.* **2016**, *6*, 31. [CrossRef]
4. Cram, W.A.; Brohman, K.; Gallupe, R.B. Information systems control: A review and framework for emerging information systems processes. *J. Assoc. Inf. Syst.* **2016**, *17*, 2. [CrossRef]
5. Sousa, V. A Review on Cyber Attacks and Its Preventive Measures. In Proceedings of the Digital Privacy and Security Conference, Porto, Portugal, 16 January 2019 ; Volume 92.
6. Bojanc, R.; Jerman-Blažič, B. An economic modelling approach to information security risk management. *Int. J. Inf. Manag.* **2008**, *28*, 413–422. . [CrossRef]
7. Dubois, É.; Heymans, P.; Mayer, N.; Matulevičius, R. A Systematic Approach to Define the Domain of Information System Security Risk Management. In *Intentional Perspectives on Information Systems Engineering*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 289–306. [CrossRef]
8. International Organization for Standardization. ISO/IEC Guide 73:2009—Risk management—Vocabulary. 2009. Available online: https://www.iso.org/standard/44651.html (accessed on 15 October 2022).
9. Knight, K.W. AS/NZS ISO 31000: 2009-the new standard for managing risk. *Keep. Good Co.* **2010**, *62*, 68.
10. Mellado, D.; Blanco, C.; Sánchez, L.E.; Fernández-Medina, E. A systematic review of security requirements engineering. *Comput. Stand. Interfaces* **2010**, *32*, 153–165. [CrossRef]
11. Khan, N.F.; Ikram, N. Security Requirements Engineering: A Systematic Mapping (2010-2015). In Proceedings of the 2016 International Conference on Software Security and Assurance (ICSSA), St. Pölten, Austria, 24–25 August 2016. [CrossRef]
12. Basin, D.; Doser, J.; Lodderstedt, T. Model driven security for process-oriented systems. In Proceedings of the Eighth ACM Symposium on Access Control Models and Technologies—SACMAT'03, Como Italy, 2–3 June 2003; ACM Press: New York, NY, USA, 2003. [CrossRef]
13. Basin, D.; Doser, J.; Lodderstedt, T. Model driven security. *ACM Trans. Softw. Eng. Methodol.* **2006**, *15*, 39–91. [CrossRef]
14. Toval, A.; Nicolás, J.; Moros, B.; García, F. Requirements Reuse for Improving Information Systems Security: A Practitioner's Approach. *Requir. Eng.* **2002**, *6*, 205–219. [CrossRef]
15. Alberts, C.J.; Dorofee, A.J. *OCTAVE Method Implementation Guide Version 2.0. Volume 1: Introduction*; Technical Report; Software Engineering Institute, Carnegi Mellon: Pittsburgh, PA, USA, 2001. [CrossRef]

16. Vraalsen, F.; Mahler, T. Assessing enterprise risk level: The CORAS approach. In *Advances in Enterprise Information Technology Security*; IGI Global: Pennsylvania, PA, USA, 2007; pp. 311–333.
17. International Organization for Standardization. ISO/IEC 27001:2013—Information Security Management. 2013. Available online: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm (accessed on 15 October 2022).
18. National Institute of Standards and Technology (NIST). 2017. Cybersecurity. Available online: https://www.nist.gov/topics/cybersecurity (accessed on 15 October 2022).
19. ISACA. Control Objectives for Information and Related Technologies (COBIT). 2017. Available online: http://www.isaca.org/Knowledge-Center/cobit/Pages/Products.aspx (accessed on 20 December 2018).
20. Whitman, M.E.; Mattord, H.J. *Principles of Information Security*; Cengage Learning: Boston, MA, USA, 2021.
21. Singh, A.N.; Gupta, M.; Ojha, A. Identifying factors of "organizational information security management". *J. Enterp. Inf. Manag.* **2014**, *27*, 644–667. [CrossRef]
22. Stoll, M. An information security model for implementing the new ISO 27001. In *Handbook of Research on Emerging Developments in Data Privacy*; IGI Global: Pennsylvania, PA, USA, 2015; pp. 216–238.
23. Chang, S.E.; Ho, C.B. Organizational factors to the effectiveness of implementing information security management. *Ind. Manag. Data Syst.* **2006**, *11*, 345–361. [CrossRef]
24. Ali, R.F.; Dominic, P.D.D.; Ali, S.E.A.; Rehman, M.; Sohail, A. Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance. *Appl. Sci.* **2021**, *11*, 3383. [CrossRef]
25. Hevner, A.; Chatterjee, S. *Design Science Research in Information Systems*; Integrated Series in Information Systems; Management Information Systems Research Center, University of Minnesota: Minneapolis, MN, USA, 2010; pp. 9–22. [CrossRef]
26. Wieringa, R. Design science as nested problem solving. In Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology—DESRIST'09, Philadelphia, PA, USA, 7–8 May 2009; ACM Press: New York, NY, USA, 2009. [CrossRef]
27. Easterbrook, S.; Singer, J.; Storey, M.A.; Damian, D. Selecting Empirical Methods for Software Engineering Research. In *Guide to Advanced Empirical Software Engineering*; Springer: London, UK, 2008; pp. 285–311. [CrossRef]
28. Diéguez, M.; Sepúlveda, S.; Cachero, C. UMAM-Q: An instrument to assess the intention to use software development methodologies. In Proceedings of the 7th Iberian Conference on Information Systems and Technologies (CISTI 2012), Madrid, Spain, 20–23 June 2012; pp. 1–6.
29. Disterer, G. ISO/IEC 27000, 27001 and 27002 for Information Security Management. *J. Inf. Secur.* **2013**, *04*, 92–100. [CrossRef]
30. International Organization for Standardization. ISO/IEC 19011:2018—Guidelines for Auditing Managementsystems. 2018. Available online: https://www.iso.org/obp/ui#iso:std:iso:19011:ed-3:v1:es (accessed on 15 October 2022).
31. Diéguez, M.; Bustos, J.; Cares, C. Mapping the variations for implementing information security controls to their operational research solutions. *Inf. Syst.-Bus. Manag.* **2020**, *18*, 157–186. [CrossRef]
32. Bistarelli, S.; Fioravanti, F.; Peretti, P. Using CP-nets As a Guide for Countermeasure Selection. In Proceedings of the 2007 ACM Symposium on Applied Computing, SAC '07, Seoul, Korea, 11–15 March 2007; ACM: New York, NY, USA, 2007; pp. 300–304. [CrossRef]
33. Nagata, K.; Amagasa, M.; Kigawa, Y.; Cui, D. Method to Select Effective Risk Mitigation Controls Using Fuzzy Outranking. In Proceedings of the 2009 Ninth International Conference on Intelligent Systems Design and Applications, Pisa, Italy, 30 November–2 December 2009; pp. 479–484. [CrossRef]
34. Otero, A.R.; Otero, C.E.; Qureshi, A. A Multi-Criteria Evaluation of Information Security Controls Using Boolean Features. *Int. J. Netw. Secur. Its Appl.* **2010**, *2*, 1–11. [CrossRef]
35. Otero, A.R.; Ejnioui, A.; Otero, C.E.; Tejay, G. Evaluation of Information Security Controls in Organizations by Grey Relational Analysis. *Int. J. Dependable Trust. Inf. Syst.* **2011**, *2*, 36–54. [CrossRef]
36. Lv, J.J.; Wang, Y.Z. A Ranking Method for Information Security Risk Management Based on AHP and PROMETHEE. In Proceedings of the 2010 International Conference on Management and Service Science, Wuhan, China, 24–26 August 2010; pp. 1–4. . [CrossRef]
37. Khajouei, H.; Kazemi, M.; Moosavirad, S.H. Ranking information security controls by using fuzzy analytic hierarchy process. *Inf. Syst. -Bus. Manag.* **2016**, *15*, 1–19. [CrossRef]
38. Cabrera, J.S.; Reyes, A.R.L.; Lasco, C.A. Multicriteria Decision Analysis on Information Security Policy: A Prioritization Approach. *Adv. Technol. Innov.* **2020**. [CrossRef]
39. Tariq, M.I.; Tayyaba, S.; Mian, N.A.; Sarfraz, M.S.; la Hoz-Franco, E.D.; Butt, S.A.; Santarcangelo, V.; Rad, D.V. Combination of AHP and TOPSIS methods for the ranking of information security controls to overcome its obstructions under fuzzy environment. *J. Intell. Fuzzy Syst.* **2020**, *38*, 6075–6088. [CrossRef]
40. Costa, I.; Guarda, T. Information System Security Risk Priority Number: A New Method for Evaluating and Prioritization Security Risk in Information System Applying FMEA. In Proceedings of the International Conference on Information Technology and Applications, Lisbon, Portugal, 20–22 October 2022; Ullah, A.; Anwar, S.; Rocha, Á.; Gill, S., Eds.; Springer: Singapore, 2022; pp. 561–572.
41. Sawik, T. Selection of optimal countermeasure portfolio in IT security planning. *Decis. Support Syst.* **2013**, *55*, 156–164. [CrossRef]

42. Kawasaki, R.; Hiromatsu, T. Proposal of a model supporting decision-making on information security risk treatment. *Int. J. Comput. Electr. Autom. Control. Inf. Eng.* **2014**, *8*, 583–589.
43. Yevseyeva, I.; Basto-Fernandes, V.; Emmerich, M.; van Moorsel, A. Selecting Optimal Subset of Security Controls. *Procedia Comput. Sci.* **2015**, *64*, 1035–1042. [CrossRef]
44. Shahpasand, M.; Shajari, M.; Golpaygani, S.A.H.; Ghavamipoor, H. A comprehensive security control selection model for inter-dependent organizational assets structure. *Inf. Comput. Secur.* **2015**, *23*, 218–242. [CrossRef]
45. Almeida, L.; Respício, A. Decision support for selecting information security controls. *J. Decis. Syst.* **2018**, *27*, 173–180. [CrossRef]
46. Zhang, H.; Chari, K.; Agrawal, M. Decision support for the optimal allocation of security controls. *Decis. Support Syst.* **2018**, *115*, 92–104. [CrossRef]
47. Ojamaa, A.; Tyugu, E.; Kivimaa, J. Pareto-optimal situaton analysis for selection of security measures. In Proceedings of the MILCOM 2008—2008 IEEE Military Communications Conference, San Diego, CA, USA, 16–19 November 2008; pp. 1–7. [CrossRef]
48. Yang, Y.P.; Shieh, H.M.; Leu, J.D.; Tzeng, G.H. A VIKOR-based multiple criteria decision method for improving information security risk. *Int. J. Inf. Technol. Decis. Mak.* **2009**, *8*, 267–287. [CrossRef]
49. Chen, L.; Li, L.; Hu, Y.; Lian, K. Information Security Solution Decision-Making Based on Entropy Weight and Gray Situation Decision. In Proceedings of the 2009 Fifth International Conference on Information Assurance and Security, 18–20 August 2009; Xi'an, China. [CrossRef]
50. Cuihua, X.; Jiajun, L. An Information System Security Evaluation Model Based on AHP and GRAP. In Proceedings of the 2009 International Conference on Web Information Systems and Mining, Shanghai, China, 7–8 November 2009; pp. 493–496. [CrossRef]
51. Gao, C.; Li, Z.; Song, H. Security Evaluation Method Based on Host Resource Availability. In Proceedings of the 2009 Third International Conference on Multimedia and Ubiquitous Engineering, Qingdao, China, 4–6 June 2009; pp. 499–504. [CrossRef]
52. Lv, J.J.; Zhou, Y.S.; Wang, Y.Z. A Multi-criteria Evaluation Method of Information Security Controls. In Proceedings of the 2011 Fourth International Joint Conference on Computational Sciences and Optimization, Kunming, China, 15–19 April 2011; pp. 190–194. [CrossRef]
53. Rees, L.P.; Deane, J.K.; Rakes, T.R.; Baker, W.H. Decision support for Cybersecurity risk planning. *Decis. Support Syst.* **2011**, *51*, 493–505. [CrossRef]
54. Yameng, C.; Yulong, S.; Jianfeng, M.; Xining, C.; Yahui, L. AHP-GRAP Based Security Evaluation Method for MILS System within CC Framework. In Proceedings of the 2011 Seventh International Conference on Computational Intelligence and Security, Sanya, China, 3–4 December 2011; pp. 635–639. [CrossRef]
55. Kiesling, E.; Strausss, C.; Stummer, C. A Multi-objective Decision Support Framework for Simulation-Based Security Control Selection. In Proceedings of the 2012 Seventh International Conference on Availability, Reliability and Security, Prague, Czech Republic, 20–24 August 2012. [CrossRef]
56. Viduto, V.; Maple, C.; Huang, W.; López-Peréz, D. A novel risk assessment and optimisation model for a multi-objective network security countermeasure selection problem. *Decis. Support Syst.* **2012**, *53*, 599–610. [CrossRef]
57. Breier, J.; Hudec, L. New approach in information system security evaluation. In Proceedings of the 2012 IEEE First AESS European Conference on Satellite Telecommunications (ESTEL), Rome, Italy, 2–5 October 2012; pp. 1–6. [CrossRef]
58. Otero, A.R.; Tejay, G.; Otero, L.D.; Ruiz-Torres, A.J. A fuzzy logic-based information security control assessment for organizations. In Proceedings of the 2012 IEEE Conference on Open Systems, Kuala Lumpur, Malaysia, 21–24 October 2012, pp. 1–6. [CrossRef]
59. Ejnioui, A.; Otero, A.R.; Tejay, G.; Otero, C.; Qureshi, A. A Multi-attribute Evaluation of Information Security Controls in Organizations Using Grey Systems Theory. In Proceedings of the International Conference on Security and Management (SAM), Las Vegas, NV, USA, 16–19 July 2012; pp. 1–7.
60. Kiesling, E.; Ekelhart, A.; Grill, B.; Strauß, C.; Stummer, C. Simulation-based optimization of IT security controls: Initial experiences with meta-heuristic solution procedures. In Proceedings of the Workshop of the EURO Working Group on Metaheuristics Hamburg, Germany, 28 February–1 March 2013; pp. 18–20.
61. Kiesling, E.; Strauss, C.; Ekelhart, A.; Grill, B.; Stummer, C. Simulation-based optimization of information security controls: An adversary-centric approach. In Proceedings of the 2013 Winter Simulations Conference (WSC), Washington, DC, USA, 8–11 December 2013; pp. 2054–2065. [CrossRef]
62. Breier, J.; Hudec, L. On Selecting Critical Security Controls. In Proceedings of the 2013 International Conference on Availability, Reliability and Security, Regensburg, Germany, 2–6 September 2013; pp. 582–588. [CrossRef]
63. Breier, J.; Hudec, L. On Identifying Proper Security Mechanisms. In *Lecture Notes in Computer Science*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 285–294. ._29. [CrossRef]
64. Yang, Y.P.O.; Shieh, H.M.; Tzeng, G.H. A VIKOR technique based on DEMATEL and ANP for information security risk control assessment. *Inf. Sci.* **2013**, *232*, 482–500. [CrossRef]
65. Breier, J. Security evaluation model based on the score of security mechanisms. *Inf. Sci. Technol.* **2014**, *6*, 19–27.
66. Al-Safwani, N.; Hassan, S.; Katuk, N. A multiple attribute decision making for improving information security control assessment. *Int. J. Comput. Appl.* **2014**, *89*, 19–24. [CrossRef]
67. Choo, K.K.; Mubarak, S.; Mani, D. Selection of information security controls based on AHP and GRA. In Proceedings of the Pacific Asia Conference on Information Systems, Chengdu, China, 24–28 June 2014.

68. Meng, M.; Liu, E. The Application Research of Information Security Risk Assessment Model Based on AHP Method. *J. Adv. Inf. Technol.* **2015**, 201–206. [CrossRef]
69. Sarala, R.; Zayaraz, G.; Vijayalakshmi, V. Optimal Selection of Security Countermeasures for Effective Information Security. In *Proceedings of the International Conference on Soft Computing Systems*; Springer: New Delhi, India, 2015; pp. 345–353. [CrossRef]
70. Ganin, A.A.; Quach, P.; Panwar, M.; Collier, Z.A.; Keisler, J.M.; Marchese, D.; Linkov, I. Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management. *Risk Anal.* **2017**, *40*, 183–199. [CrossRef]
71. Fenz, S.; Neubauer, T. Ontology-based information security compliance determination and control selection on the example of ISO 27002. *Inf. Comput. Secur.* **2018**, *26*, 551–567. [CrossRef]
72. Arogundade, O.T.; Abayomi-Alli, A.; Misra, S. An Ontology-Based Security Risk Management Model for Information Systems. *Arab. J. Sci. Eng.* **2020**, *45*, 6183–6198. [CrossRef]
73. Alenezi, M.; Nadeem, M.; Agrawal, A.; Kumar, R.; Khan, R.; Fuzzy Multi Criteria Decision Analysis Method for Assessing Security Design Tactics for Web Applications. *Int. J. Intell. Eng. Syst.* **2020**, *13*, 181–196. [CrossRef]
74. Razikin, K.; Soewito, B. Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework. *Egypt. Inform. J.* **2022**, *23*, 383–404. [CrossRef]
75. Gass, S.I.; Saaty, T.L. Parametric Objective Function (Part 2)—Generalization. *J. Oper. Res. Soc. Am.* **1955**, *3*, 395–401. [CrossRef]
76. Wierzbicki, A.P. The Use of Reference Objectives in Multiobjective Optimization. In *Lecture Notes in Economics and Mathematical Systems*; Springer: Berlin/Heidelberg, Germany, 1980; pp. 468–486. [CrossRef]
77. Cheng, T.; Ng, C.; Yuan, J.; Liu, Z. Single machine scheduling to minimize total weighted tardiness. *Eur. J. Oper. Res.* **2005**, *165*, 423–443. [CrossRef]
78. Koulamas, C. The single-machine total tardiness scheduling problem: Review and extensions. *Eur. J. Oper. Res.* **2010**, *202*, 1–7. [CrossRef]
79. Edis, E.B.; Oguz, C.; Ozkarahan, I. Parallel machine scheduling with additional resources: Notation, classification, models and solution methods. *Eur. J. Oper. Res.* **2013**, *230*, 449–463. [CrossRef]
80. Wäscher, G.; Haußner, H.; Schumann, H. An improved typology of cutting and packing problems. *Eur. J. Oper. Res.* **2007**, *183*, 1109–1130. [CrossRef]
81. Egeblad, J.; Pisinger, D. Heuristic approaches for the two- and three-dimensional knapsack packing problem. *Comput. Oper. Res.* **2009**, *36*, 1026–1049. [CrossRef]
82. Florios, K.; Mavrotas, G.; Diakoulaki, D. Solving multiobjective, multiconstraint knapsack problems using mathematical programming and evolutionary algorithms. *Eur. J. Oper. Res.* **2010**, *203*, 14–21. [CrossRef]
83. Ghasemi, T.; Razzazi, M. Development of core to solve the multidimensional multiple-choice knapsack problem. *Comput. Ind. Eng.* **2011**, *60*, 349–360. [CrossRef]
84. Wang, L.; Wang, S.Y.; Xu, Y. An effective hybrid EDA-based algorithm for solving multidimensional knapsack problem. *Expert Syst. Appl.* **2012**, *39*, 5593–5599. [CrossRef]
85. Hartmann, S.; Briskorn, D. A survey of variants and extensions of the resource-constrained project scheduling problem. *Eur. J. Oper. Res.* **2010**, *207*, 1–14. [CrossRef]
86. Tasan, S.O.; Gen, M. An integrated selection and scheduling for disjunctive network problems. *Comput. Ind. Eng.* **2013**, *65*, 65–76. [CrossRef]
87. Samphaiboon, N.; Yamada, Y. Heuristic and Exact Algorithms for the Precedence-Constrained Knapsack Problem. *J. Optim. Theory Appl.* **2000**, *105*, 659–676. . [CrossRef]
88. Samavati, M.; Essam, D.; Nehring, M.; Sarker, R. A methodology for the large-scale multi-period precedence-constrained knapsack problem: An application in the mining industry. *Int. J. Prod. Econ.* **2017**, *193*, 12–20. [CrossRef]
89. Espinoza, D.; Goycoolea, M.; Moreno, E. The precedence constrained knapsack problem: Separating maximally violated inequalities. *Discret. Appl. Math.* **2015**, *194*, 65–80. [CrossRef]
90. Hoogeveen, H. Multicriteria scheduling. *Eur. J. Oper. Res.* **2005**, *167*, 592–623. [CrossRef]
91. Mauergauz, Y. Multi-criteria Models and Decision-Making. In *Advanced Planning and Scheduling in Manufacturing and Supply Chains*; Springer International Publishing: Berlin/Heidelberg, Germany, 2016; pp. 127–162. [CrossRef]
92. International Organization for Standardization. ISO/IEC 27002:2013—Information Technology—Security Techniques—Code of Practice for Information Security Controls. 2013. Available online: http://www.iso.org/iso/catalogue_detail?csnumber=54533 (accessed on 15 October 2022).
93. gams Development Corporation. General Algebraic Modeling System. 2017. Available online: http://www.gams.com/ (accessed on 15 October 2022)
94. Wisconsin Institutes for Discovery. NEOS Server for Optimization Web Portal. Available online: http://www.neos-server.org/neos/ (accessed on 15 October 2022).

95. Gobierno de Chile. Decreto 83: Norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos. Available online: http://www.leychile.cl/Navegar?idNorma=234598 (accessed on 15 October 2022).
96. Gobierno de Chile. Programa de mejoramiento de la gestión sistema de seguridad de la información: Versión 2011. Available online: http://www.dipres.gob.cl/594/w3-propertyvalue-16887.html (accessed on 15 October 2022).