Dynamic Cybersecurity Model based on ISO standards for Higher Education Institutions in Colombia

Modelo Dinámico de Ciberseguridad basado en estándares ISO para las Instituciones de Educación Superior en Colombia

Modelo Dinâmico de Cibersegurança baseado em padrões ISO para Instituições de Ensino Superior na Colômbia

María Alejandra Varona Taborda[1]
Fabian Alexander Montano Collazos[2]
Carlos Alejandro Escobar Marulanda[3]
Katerine Márceles Villalba[4]

Received: May 25th, 2021
Accepted: August 20th, 2021
Available: September 6th, 2021

How to cite this article:
M.A Varona Taborda, F.A. Montano Collazos, C.A. Escobar Marulanda, K. Márceles Villalba "Dynamic Cybersecurity Model based on ISO standards for Higher Education Institutions in Colombia," *Revista Ingeniería Solidaria,* vol. 17, no. 3, 2021.
doi: https://doi.org/10.16925/2357-6014.2021.03.05

Research article. https://doi.org/10.16925/2357-6014.2021.03.05

[1] Master's Program in Information Technology Management, Faculty of Engineering, Tecnológico de Antioquia University Institution, Medellín, Colombia.
Email: mvarona@unimayor.edu.co
ORCID: https://orcid.org/0000-0001-9545-4766

[2] Master's Program in Information Technology Management, Faculty of Engineering, Tecnológico de Antioquia University Institution, Medellín, Colombia.
Email: fabianmontano@unimayor.edu.co
ORCID: https://orcid.org/0000-0002-2982-6549

[3] Master's Program in Information Technology Management, Faculty of Engineering, Tecnológico de Antioquia University Institution, Medellín, Colombia.
Email: ealejandro101@gmail.com
ORCID: https://orcid.org/0000-0002-6818-1296

[4] Computer Engineering Program, Faculty of Engineering, Colegio Mayor del Cauca University Institution, Popayán, Colombia.
Email: kmarceles@unimayor.edu.co
ORCID: https://orcid.org/0000-0002-4571-0714

Abstract

Introduction: This article is the result of a research process whose product was to generate a guide for Higher Education Institutions (in Spanish, IES) to adopt a Cybersecurity Model based on ISO standards (International Organization for Standardization).

Problem: IES do not have a cybersecurity model aligned to the ISO / IEC 27032: 2012 standard (International Organization for Standardization / International Electrotechnical Commission), which causes a lack of clarity and uncertainty in the level of maturity and a low efficiency in the processes and information security controls to be implemented.

Objective: Propose a dynamic model of cybersecurity based on ISO standards for IES.

Methodology: The development of this work was oriented under a line of applied research.

Results: A dynamic model that can be adapted to the different needs and requirements of IES has been generated.

Conclusion: IES can implement a cybersecurity model to prevent and protect information at the cyberspace level.

Originality: At present there are no specific dynamic cybersecurity models for IES.

Limitations: The model implementation guide is established in a general way to be applied later to an organization in any sector.

Keywords: Dynamic Cybersecurity Model, Higher Education Institutions, ISO/IEC 27032: 2012, Security Standards.

Resumen

Introducción: Este artículo es resultado de un proyecto de investigación "Modelo dinámico de ciberseguridad basado en estándares ISO para IES" desarrollado en el Tecnológico de Antioquia Institución Universitaria en el año 2020, cuyo producto fue generar una guía para que las IES (Instituciones de Educación Superior) puedan adoptar un Modelo de Ciberseguridad basado en estándares ISO (International Organization for Standardization).

Problema: Las IES no cuentan con un modelo de ciberseguridad alineado al estándar ISO/IEC 27032:2012 (Internacional Organization for Standardization/International Electrotechnical Commission), lo que ocasiona falta de claridad e incertidumbre en el nivel de madurez y baja eficiencia en los procesos y los controles de seguridad de la información que se deben implementar.

Objetivo: Proponer un Modelo dinámico de ciberseguridad basado en estándares ISO para las IES.

Metodología: El desarrollo de este trabajo se orientó bajo una línea de la investigación aplicada, en virtud de que se vió necesario abordar el problema a partir de conocimientos previos que permitieron soportar los aportes teóricos y las actividades propuestas para determinar las posibles causas del problema y darle una posible solución.

Resultados: La generación de este modelo dinámico permite que pueda adaptarse a las diferentes necesidades y requerimientos de las IES.

Conclusión: Las IES pueden implementar un modelo de ciberseguridad para prevenir y proteger la información a nivel del ciberespacio.

Originalidad: El trabajo realizado genera un gran aporte que es la generación de un modelo dinámico de ciberseguridad, dado que en la actualidad no se encuentran modelos específicos para las IES.

Limitaciones: La guía de implementación del modelo se establece de manera general para ser aplicada posteriormente a una organización de cualquier sector.

Palabras clave: Estándares de Seguridad, Instituciones de Educación Superior, ISO/IEC 27032:2012, Modelo dinámico de ciberseguridad.

Resumo

Introdução: Este artigo é o resultado de um projeto de pesquisa "Modelo dinâmico de segurança cibernética baseado em padrões ISO para IES" desenvolvido no Tecnológico de Antioquia Institución Universitaria no ano de 2020, cujo produto foi gerar um guia para que as IES (Instituições de Ensino Superior) pode adotar um Modelo de Cibersegurança baseado nas normas ISO (International Organization for Standardization).

Problema: as IES não possuem um modelo de cibersegurança alinhado com a norma ISO/IEC 27032:2012 (International Organization for Standardization/International Electrotechnical Commission), o que causa falta de clareza e incerteza no nível de maturidade e baixa eficiência nos processos e nas informações controles de segurança que devem ser implementados.

Objetivo: Propor um modelo dinâmico de cibersegurança baseado em padrões ISO para IES.

Metodologia: O desenvolvimento deste trabalho foi orientado sob uma linha de pesquisa aplicada, em virtude do fato de ser necessário abordar o problema a partir de conhecimentos prévios que permitissem subsidiar os aportes teóricos e as atividades propostas para determinar as possíveis causas do problema. e dar-lhe uma solução possível.

Resultados: A geração deste modelo dinâmico permite adaptá-lo às diferentes necessidades e exigências das IES.

Conclusão: As IES podem implementar um modelo de cibersegurança para prevenir e proteger a informação ao nível do ciberespaço.

Originalidade: O trabalho realizado gera uma grande contribuição, que é a geração de um modelo dinâmico de cibersegurança, visto que atualmente não existem modelos específicos para IES.

Limitações: O guia de implementação do modelo é estabelecido de forma geral para ser aplicado posteriormente a uma organização de qualquer setor.

Palavras-chave: Normas de Segurança, Instituições de Ensino Superior, ISO/IEC 27032:2012, Modelo dinâmico de cibersegurança.

1. INTRODUCTION

It is imperative that Higher Education Institutions (IES) establish new challenges in the context of cybersecurity and cyberdefense. Before it was only enough to know and understand the threats known from the environment; now, updated or new proposals must be configured that, in addition to protecting and securing information assets, anticipate and defend against unknown or uncertain scenarios, that enable organizations and countries to identify and manage latent and emerging risks with a more systemic view [1]. For this reason, it is important that IES strengthen their processes with a dynamic cybersecurity model based on the ISO / IEC 27032: 2012

cybersecurity standard, which will facilitate the implementation of security controls and thus prevent problems in the integrity, availability and reliability of information.

1.1 Conceptual aspects

Analysis of Cybersecurity in Colombian organizations with regards to Cybercrime trends in Colombia [2], between the Colombian Chamber of Informatics and Telecommunications and the reports made by companies and citizens to the CECIP Police Cybernetic Center, presents the different types of attack to which organizations are exposed. The analysis, encompassing 15 948 complaints and reports from the most reported incidents in Colombia can be categorized as folloews: 42% phishing cases , 28% identity theft, 14% sending malware and 16% fraud in online payment methods, where the main interest of cybercriminals is financial and subsequent monetization of the profits generated in each Cyber-attack. Among the most common computer crimes in the country are: computer theft, the violation of personal data, abusive access to the computer systems, the non-consensual transfer of assets and the use of Malicious Software. In turn, social engineering is responsible for 90% of company cyber threats. For this reason, the importance of strengthening cybersecurity models is evident and the dissemination of the appropriate knowledge on how to safeguard the information of the data that are constantly exposed internally and externally in cyberspace is of utmost importance. Some of the most common attacks currently being used include: the corporate email spoofing attack BEC (Business Email Compromise), cryptocurrency mining, ransomware, denial of service attacks, malware, SIM card hijacking or change and Cryptojacking [2].

Organizations seek to protect cyber assets and implement cybersecurity measures and programs, but despite this ongoing effort, cybersecurity breaches and cyber attacks inevitably occur [3].

A cybersecurity model is the representation of a concept or process through defined variables to achieve a better understanding following pre-established parameters to measure and validate cybersecurity issues based on established norms, policies, and standards.

The construction of a model involves the following steps:

Carry out an Investigation on legislation: Where the information security protection laws determined by the Country, organization, or company with which you are going to work must be established and identified.

Define the importance and benefits that will be obtained with the model to socialize them with the stakeholders of the organization or company with which you are going to work.

Establish cybersecurity objectives with clear and quantifiable objectives.

Choose the reference framework for the implementation of cybersecurity among which are the cybersecurity standard ISO / IEC 27032: 2012, COBIT (Control Objectives for Information and related Technology) that can be defined as a guide or model to perform audits of the management and control of information and technology systems, aimed at the IT departments of an organization; that is, the auditors involved in the process [4] and the NIST SP 800-53 Cybersecurity Framework that represents the security controls and defined assessment procedures.

1.2 Literature review or research background

In [5], they present the difference from the rest of the environments where cyberattacks are fought; cyberspace has a physical and virtual dimension, thus, any event that occurs in cyberspace has effects on the physical world and vice versa. In particular, the lack of cybersecurity measures in public Higher Education Institutions can generate some problems, which grow over time, and as the probability of being the target of computer attacks increases, the greater is the impact of risk. To control more security in cyberspace, there are regulations that regulate and help to improve this type of problem, such as the ISO/IEC 27032: 2012 Cybersecurity Guidelines, and those that contribute to risk mitigation, such as the Modal Analysis of Failures and Effects (AMFE) methodology; they are applied when designing new products, services, or processes. To complement the execution of this research, in the discovery of the vulnerabilities in the distributed systems of the public IES of Manabí, vulnerability scanning tools such as Shodan, Nessus, and Acunetix were applied, which scanned the public IP, or by link web of the systems of the public IES of Manabí, where it was possible to obtain the already classified vulnerabilities. Once the previous process was finished, the preparation of the action plan continued, taking into account the mitigation strategies and acceptance criteria of the AMFE risk matrix, thereby improving the security of the distributed systems of these public institutions and in this way, reduce the risks encountered. This is one of the most relevant studies within the literature, providing a model example of cybersecurity applied to Higher Education Institutions.

[3] presents the results of an implementation and validation study of the Cybersecurity Audit Model (CSAM), it is an innovative and comprehensive model that includes the evaluation of cybersecurity in any organization and can review specific guidelines for nations that wish to implement a cybersecurity strategy. The CSAM can be implemented to run cybersecurity audits on an individual basis or it can be part of

a general audit implementation to improve organizational controls. The main objective is to introduce a cybersecurity auditing model that can include all functional areas, in order to generate an effective evaluation of cybersecurity, its maturity and cybernetic readiness in any organization or nation that is auditing.

The study carried out by Sisteseg Consulting Services [6], provides information of great importance in the context related to the implementation of the ISO 27032: 2012 Standard, serving as a guide in the development of this project, as well as a reference framework in comparing cybersecurity models proposed.

[7] proposes cybersecurity standards focused on MSMEs: IASME (Information Assurance for Small and Medium Sized Enterprises) is a standard created by the IASME consortium made up of an academic entity (University of Worcester), private cybersecurity consultants and an association of IT professionals (National Computing Center), ISSA-UK 5173 (Information Systems Security Association) is an international non-profit organization dedicated to connecting the various professionals in cybersecurity worldwide. They also deal with the analysis and choice and comparison of different maturity models, which help to develop the comparative of the models in the project [29] [30].

In [8], the authors addresses information as a key element in the development and success of companies; for that reason, organizations are more aware of the need to protect information from the threats to which they are exposed. It should be taken into account that there are many different types of threats that affect information systems and their information in general. Not all of them are related to computer crimes, but for the most part, they are a risk for organizations and their effects must be evaluated: Possible software and / or hardware failures, environmental and / or natural events, accidents, previously planned threats of an entirely criminal nature such as theft or destruction of property, and general threats of external and / or internal origin. As such, this document considers the different computer threats that occur in organizations and presents them in a general way, being a frame of reference to carry out the instrument to be applied [28].

[9] provides information related to the legal aspects in computer security that must be taken into account in organizations. In current environments, there are multiple norms and standards that provide guides to best practices with proposals related to and executed on the security of the area of IT. These standards define policies, processes, controls and actions. The drawback is that the incoherence of the information that is handled within organizations, added to the growing number of threats, complicates the diagnosis required for a clear image of the strengths and weaknesses, as well as the action plans to be executed.

[10] brings into context the importance of keeping an organizations' data safe. To do so, it is necessary to comply with three fundamental pillars of information security: Availability, information must be at hand and always available for those who need access, that is, by personnel who are previously authorized either for modification or for reading; Integrity, the information that is possessed must not be altered and must be kept exactly how it was generated and; Confidentiality, information is only available to people or applications and processes that have authorization.

[11] establishes a reference model in the implementation of information security policies based on the guidelines provided by international norms and standards, among which are ISO 17799, COBIT, ITIL (Information Technology Infrastructure Library), LEY SOX (Sarbanes Oxley Act), COSO (Committee of Sponsoring Organizations of the Treadway) and ISO 27000 Series. In this study, phases and activities that are part of this model are established: detection of needs, risk analysis, directive support, official of information security, Preparation of ISP (Information Security Policies), preparation of procedures, instructions and records, IT controls, evaluation and audit, evidence, reports, action plans and awareness, the contribution to this project is established by the different norms and reference standards and the aspects to be taken into account related to the development phases.

2. MATERIALS AND METHODS

This article is developed within the lines of applied research [12] that works with previous knowledge that is supported in theoretical contributions and activities which will allow to determine the possible causes of the problem posed and thus demonstrate them. This in turn will allow, together with the research results, to generate a practical document that will propose a dynamic cybersecurity model that can be adapted in different IES.

Therefore, the following general guide is proposed, which will lead to the formulation of the specific security model for an IES:

Phase 1: Review the state of the art on cybersecurity models that may be a reference for the creation of the proposed model.

Phase 2: Establish a comparative table of the selected models based on the established indicators.

Phase 3: Define the contributions obtained for the construction of the new model, after the analysis of the different models: the most important points of the results are extracted from the comparison to build a new model.

Phase 4: Build a dynamic cybersecurity model based on ISO standards.

Phase 5: Graphically design the structure of the Cybersecurity model: within the design, the standards that will be worked with the model will be adjusted and the entire structure of the new model graphically represented.

Phase 6: Evaluation of the model from a validated instrument based on reliability, validity, and objectivity.

3. RESULTS

This chapter presents the development of each of the established phases.

Phase 1: Review the state of the art on cybersecurity models that may be references for the creation of the proposed model.

A sample of existing cybersecurity models is selected and defined based on established indicators.

Among the references that were selected, [6] is a study that establishes that in the field of information security, according to ISO 27032: 2012, it is necessary to have a security model that facilitates the implementation of security controls. The model presented in this study seeks to allow the effective and efficient implementation of the standard, since documentation is a fundamental part of the entire process and recommends relying on its model to achieve the goal of protecting information. The main components of this model are objectives, policies, procedures, and configuration standards as can be seen in Figure 1.

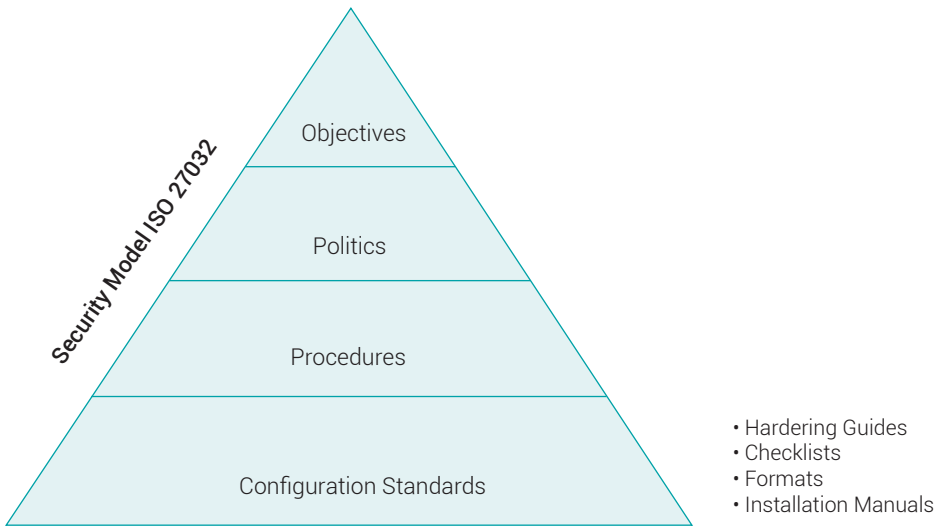

Figure 1. Levels of Model Implementation
Source: Taken from [6]

e-ISSN 2357-6014 / Vol. 17, no. 3 / september-december 2021 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

Referencing [13], different aspects related to the Standard are taken into account:

1. Scope
2. Applicability
3. Description
4. References
5. Terms of Service
6. Abbreviations
7. Generalities
8. Stakeholders in Cyberspace
9. Assets in Cyberspace
10. Cyberspace security threats
11. Roles of stakeholders in Cybersecurity
12. Guidelines for stakeholders in Cybersecurity Controls
13. Information exchange and coordination framework

In [5], a cybersecurity analysis was carried out with the elaboration of questionnaires (checklists) based on the ISO / IEC 27032: 2012 standard, with the domains related to information, network and application security; it should be noted that in this case the control related to Social Engineering was not taken into account. In this study, the quantitative method was applied, which quantified the data using the Likert scale, where 4 is a non-vulnerable process, 3 is not very vulnerable, 2 vulnerable and 1 very vulnerable. In the process of identifying the risks of each of the vulnerabilities found through the checklist data, the AMFE matrix was prepared for each domain of the applied standard, determined by: the probability of occurrence and the impact, the level of risk of the vulnerabilities, issuing mitigation actions and acceptance criteria, thereby providing an improvement proposal. This was followed by the application of vulnerability scanning tools such as Shodan, Nessus, and Acunetix, which scanned the public IP, or by web link of the systems of the public IES of Manabí, where it was possible to obtain the already classified vulnerabilities. Finally, an action plan was developed, taking into consideration the mitigation strategies and acceptance criteria of the AMFE risk matrix, improving the security of the distributed systems of these public institutions and thus, reducing the risks encountered.

In [3], different contributions related to cybersecurity models can be established to meet challenges that may arise when planning and conducting cybersecurity audits; As well as the implementation of the training of cybersecurity awareness, this study shows the CSAM (Cybersecurity Audit Model), which is not exclusive to an industry,

sector or organization; therefore, it can be used to plan, carry out and verify audits of cybersecurity in any organization or country, where all functional areas are included, in order to ensure an effective evaluation of cybersecurity, its maturity and cybernetic readiness. The study specifies the structure of the model, the work methodology and the possible options for implementation, establishing the domains, subdomains, controls, checklists, guideline assessment, and scorecard.

Phase 2: Establish a comparative table of the selected models based on the established indicators.

The comparative table of cybersecurity models is established, referencing some studies that will allow for the analysis of different characteristics of each one and establish the contributions that will determine the design of the dynamic cybersecurity model, as evidenced below in Table 1.

Table 1. Comparative table of cybersecurity models based on indicators.

Indicator	"Implementing the ISO 27032: 2012 Standard"	"Cybersecurity and its application in Higher Education Institutions"	Cybersecurity Audits: A General Application Model for Companies and Nations	
Case study	• Organizations and Institutions	• Higher Education Institutions	• Business	
Domains / Controls	• App controls • Server controls End user controls • Social Engineering controls	• information • Applications • Networking	• Nations • Governance and Strategy • Legal framework and compliance • Cyber Assets • Cyber Risks • Frameworks and Regulations • Architecture and Networks • Information, Systems and Applications • Identification of Vulnerabilities	• Threat Intelligence • Incident Management • Digital Forensic Analysis • Awareness Education • Cyber insurance • Active Cyber Defense • Evolutionary Technologies • Disaster recovery • Human resources management
Assessment instrument	• Interviews	• ISO 27032: 2012 Checklist analysis	• Checklists	
Evaluation Methodology	• GAP maturity level • Complexity: High, Half, Low	• Quantitative method • Likert scale • Very vulnerable 1 • Vulnerable 2 • Little vulnerable 3 • It is a non-vulnerable process 4	• Immature (I): 0-30 • In development (D): 31-70 • Mature (M): 71-90 • Advanced (A): 91-100	

Source: own work

e-ISSN 2357-6014 / Vol. 17, no. 3 / september-december 2021 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

In Table 1, the similarities and differences of each of the cybersecurity models are shown. It can be established that the three models can be applied in institutions, organizations and companies, different domains and controls are presented, the different instruments used for evaluation are also shown and, finally, the evaluation methodology of each one.

Phase 3: Define the contributions obtained for the construction of the new model, after analyzing the different models: the most important points of the results are extracted from the comparison to build a new model.

After analyzing the different studies that were established as a reference, some important aspects of these were taken and new ones were built in accordance with the ISO / IEC 27032: 2012 Standard.

When examining Table 1, the controls that conform to the new model based on the ISO / IEC 27032: 2012 Standard were defined. Referencing the first study called "Implementing the ISO 27032: 2012 Standard", it can be established that these 4 controls are adjusted to the needs of the new model.

Among the instruments proposed in the reference models are the interview, the checklist analysis and the checklists, for which the interview-type instrument was chosen in the new model and having a specific result of the needs presented by the institution in order to carry out an improvement plan for the same instrument.

After verifying and analyzing the evaluation methodologies in the comparative table, a new methodology was generated with percentage results to be able to measure the degree of maturity that better adapts to the dynamic model that is proposed.

Phase 4: Build a dynamic cybersecurity model based on ISO standards.

In this phase, the cybersecurity model was designed based on different ISO standards.

Each of the ISO standards established in the proposed dynamic model are described below.

ISO / IEC 27032: 2012: The international organization for ISO standardization created the defined standard with the number 27032 focused entirely on cybersecurity, taking into account that it is now one of the greatest risks that organizations face today. The main objective of the standard is to guarantee and ensure the security of information during information transfers that occur in all types of networks and thus avoid hacks, sabotage or any type of alteration to the information that could corrupt it or put it at risk. This ISO [14] raises the use of best practices for information security. In addition, it proposes tools to carry out management within organizations and has processes for the protection of operations and activities that are carried out online; in the dynamic model presented, this standard is the main reference in the model.

ISO / IEC: 20000-1: It is an international standard and its objective is the global and efficient management of services, includes a group of key processes that include the management of service levels, the generation of reports, budgets and accounting of services, to the management of suppliers, incidents and problems, change management among others [15]. This standard is part of the dynamic model and when implemented it can achieve permanent control of activities and, by monitoring processes, improve the quality of its services, managing to measure and / or compare the management carried out to its clients through independent evaluations. In the same way, the Information Technology area can apply it to show effective management of its resources.

ISO / IEC 27001: The main objective of the standard is to protect the confidentiality, integrity and availability of information in organizations. This is done from an analysis of the potential problems that may affect the organization and then define the necessary parameters in order to avoid problems [16]. The controls that are implemented after identifying the risks, generally materialize in the form of policy, procedure or technical implementation. Most of the implementation of the ISO is related to the creation or delimitation of organizational rules. This ISO is important for institutions, because most of the legal requirements related to information security are fulfilled with the methodology, processes and procedure established in the standard; in addition to having a certification that validates compliance with the best practices in terms of information security standards.

ISO / IEC 27002: The main objective of the standard is to establish guidelines and principles to initiate, implement, maintain and improve the management carried out by the institutions regarding information security [17]. The advantages of having this ISO implemented include the greater control that can be obtained over information assets, reducing the risk of liability for not having an Information Security Management System implemented. According to the ISO, the acquisition of assets must be justified and, in turn, that these have an owner or manager within the organization; those owners will have the responsibility of applying the necessary controls. The employee who is responsible for an asset must have the approval of senior management to establish controls for production, development, maintenance, use, and the general safety of the asset.

The ISO proposes four fundamental control activities:

- Conduct asset inventory.
- Protect property of assets.

- Acceptable use of assets.
- Return of assets.

In this way, the ISO controls the movements of information assets; as can be seen in the model, it has been related to controls.

ISO / IEC 29119: 2013: The objective of the standard is to provide a standard for software testing, processes, documentation, techniques, and an evaluation model for software testing processes that can be adapted to the development life cycle of the software [18].

The standard consists of 5 parts:

Definitions and vocabulary: This section provides an overview of the standard and general concepts of software testing; in addition to providing a glossary of terms covering the testing of the entire software life cycle.

Test Process: The standard defines a generic process test guideline that can be adapted within any software development and life cycle.

Test documentation: It is the part of the ISO that covers the documentation of the tests in the life cycle of the software; this includes the customizable templates that cover all the test phases.

Testing Techniques: Proposes a variety of common tools and techniques for testing software.

ISO 19770-1: Establishes a framework for IT asset management processes that allows the institution to support the implementation of software asset management with standards suitable to satisfy the organization's requirements and guarantee effective support for the management of services in general. This standard may apply to software and related assets, regardless of the software [19]. As an example, it can be applied to executable software, such as: application programs, operating systems and utility programs that work within the institution; and non-executable software such as audio and video recordings, dictionaries, documents, among others.

Phase 5: Graphically design the structure of the Cybersecurity model: within the design, the standards that will be worked with the model will be adjusted and the entire structure of the new model graphically represented.

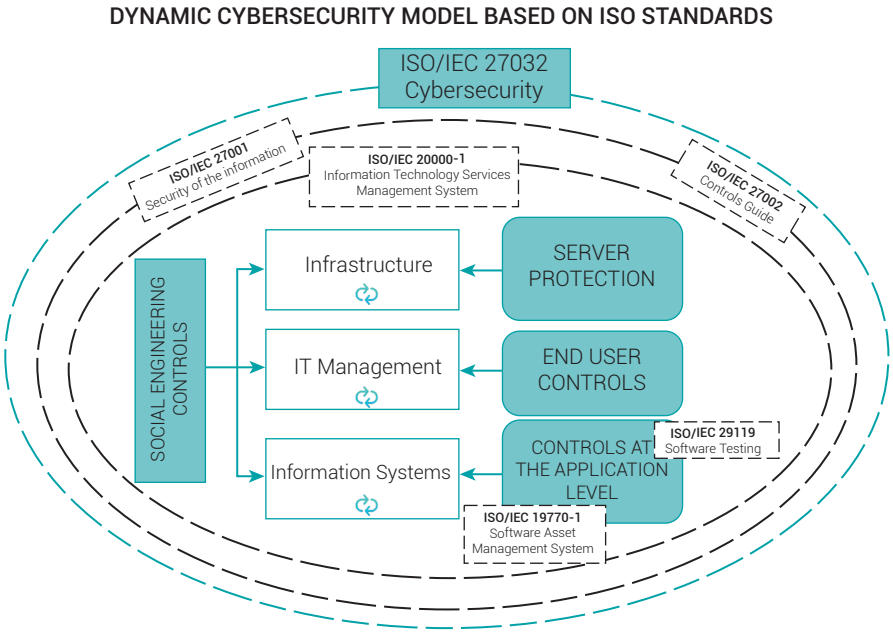

Figure 2. Dynamic Cybersecurity Model Based on ISO Standards.
Source: own work

Figure 2 represents a dynamic cybersecurity model that can be applied in different organizations and institutions, its structure considers the four cybersecurity controls established in the ISO / IEC 27032: 2012 standard, the controls against attacks from Social Engineering that are directly related to all processes, procedures and / or dependencies and the three remaining controls are directly related to one-to-one coverage, that is, a control is related to a process.

In the ISO Standards shown in Figure 2, ISO 27032:2012 is the standard that will be applied to this model and is related to the four corresponding cybersecurity controls, in the case of Infrastructure, IT Management and Information Systems. In the model, they can be adapted to the needs and requirements in different institutions as it is dynamic.

In this case, the Server Protection Controls and the Social Engineering Controls are related to Infrastructure, a process that is adapted for each institution or organization that needs to implement this model. This process refers to everything related to infrastructure: components, servers, networks, hardware, cabling, among others.

The End User Controls and the Social Engineering Controls are related to the IT Management process, a process that changes depending on each institution or organization that needs to implement this model. This process refers to the coordination,

management, administration of the IT resources, including information systems, platforms, users, vendors, and IT environments in general.

The Controls at the Application Level and the Social Engineering Controls are related to Information Systems, a process that changes depending on each institution or organization that needs to implement this model. This procedure refers to information systems, applications, software that are handled within the institutions or organizations.

Phase 6: Evaluation of the model from a validated instrument based on reliability, validity, and objectivity.

A survey-type instrument was designed, dividing the questions into four sections that correspond to each control to be evaluated: Server Protection Control, End User Control, Application Level Control and Social Engineering Controls.

The instrument used has questions of the Yes / No type or those called dichotomous items [20] and with information feedback comments related to each of the questions.

In applying the dynamic cybersecurity model, the following steps were carried out:

The first step is to adopt the cybersecurity controls in the model, at the same time, the processes, sub-processes, specific procedures or how they are handled by each institution or organization are identified and then they are directly related to each cybersecurity control.

The next step is to identify the personnel responsible for each process based on the organization chart of the institution or organization and continue with the formal presentation to them.

Continuing on from the previous step, the model must be presented to the responsible personnel to be evaluated and adapted to their needs, adjusting to the scope that is required by the institution or organization and then applying the survey instrument.

Finally, the results of the instrument are obtained by generating a percentage graph of the resulting maturity level to later be analyzed thereby leading to good cybersecurity practices.

In Figure 3, an example of the graph of the results obtained after applying the instrument is shown; a 100% objective result is expected.

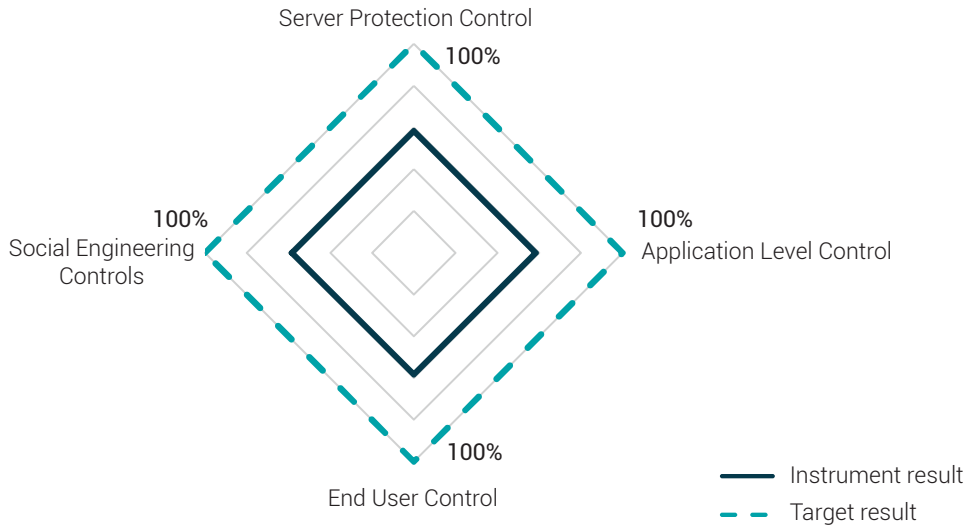

Figure 3. Example of the result after applying the Instrument.
Source: own work

In this case, it refers to the answers given by the instrument where information of great value is obtained with accurate and significant results to diagnose by measuring the procedures framed in the established cybersecurity controls. The objectivity of the instrument is generated after a previous socialization with those responsible for the procedures that allow it to be resolved in a simple way and with truthful information; in addition, to being a contribution to the institution in the strengthening processes in aspects related to Cybersecurity and the Information Security System [21, 22, 23].

To measure the validity and reliability of the instrument, the Kuder Richardson coefficient should be used [20], applied to evaluate surveys with dichotomous items. In this case the response variables Yes / No are assigned values of "1" and "0", the formula applied to the instrument is shown below [20].

$$kr_{20} = \left(\frac{K}{K-1}\right) * \left(1 - \frac{\Sigma p.q}{Vt}\right)$$

kr_{20} = Reliability Coefficient (Kuder Richardson).
K = Total number of items within the instrument.
Vt = Total Variance.
Σp.q = Sum of the Variance of the items.
p = Total of correct answers among number of participating subject.
q = 1-p

e-ISSN 2357-6014 / Vol. 17, no. 3 / september-december 2021 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

The value of the Kuder Richardson coefficient generates the degree of reliability of the instrument as shown in Table 2.

Table 2. Interpretation of the Reliability Coefficient.

RANKS	MAGNITUDE
0.81 to 1.00	Very high
0.61 to 0.80	high
0.41 to 0.60	Moderate
0.21 to 0.40	Low
0.01 to 0.20	Very low

Source: Taken from [24]

It should be noted that the dynamic cybersecurity model and the instrument were socialized and evaluated by a group of experts from an IES showing that the model can be dynamically adjusted to different sub-processes and procedures that are handled within the institution, this makes it adapt in a simple and clear way.

The group of IES collaborators came up with different suggestions and comments that helped to make small adjustments; It should be noted that they show that the model and the instrument comply with what is necessary for its measurement and being divided by procedures and by the controls to be evaluated, thus allowing for easy development.

After applying the instrument in the institution, it generated a value of 0.69 when applying the formula of the Kuder Richardson coefficient with a high degree of reliability based on Table 2.

Finally, in Figure 4, the results are displayed after applying the instrument to the personnel responsible for the IES; the data is represented in percentage of compliance with the controls analyzed.

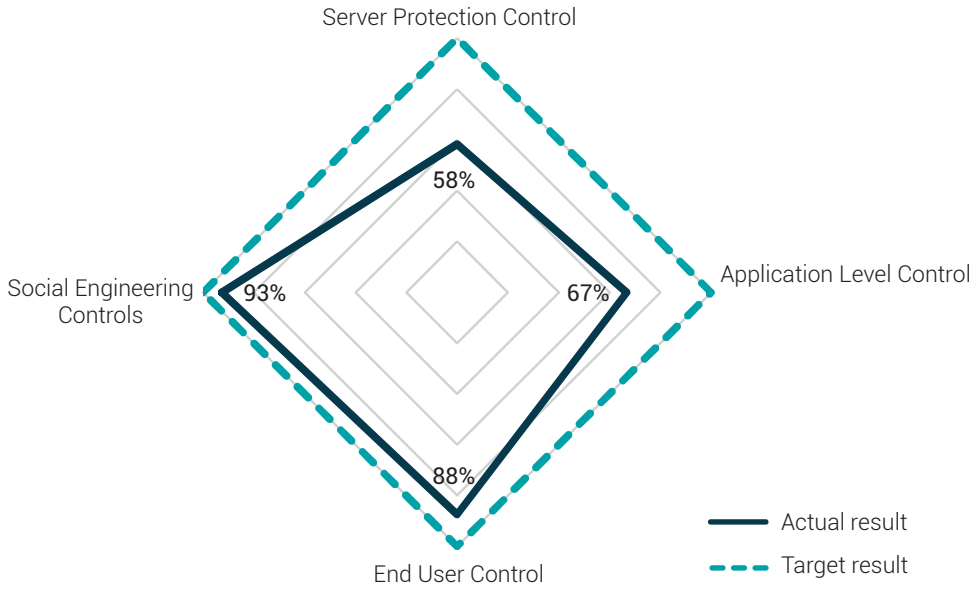

Figure 4. General result of the Assessment Instrument in the IES.
Source: own work

The Server Protection Control presents a 58% compliance in this control, which shows that it is necessary to increase protocols and have better cybersecurity practices associated with the Administration of servers and network services.

The End User Control show 88% compliance with these controls, which shows that the institution is carrying out good cybersecurity practices.

The Control at the Application Level presents a 67% compliance in this control, which shows that it is necessary to increase the protocols and have better cybersecurity practices.

The Control against Social Engineering Attack presents a 93% compliance in this control, which shows that it has good cybersecurity practices about this component.

4. DISCUSSION AND CONCLUSIONS

This study is a guide for different IES to adapt the model to their procedures, requirements and needs.

This dynamic model of cybersecurity is a great contribution since there are no specific models for IES.

IES must have a cybersecurity model in place to prevent and protect information at the cyberspace level, [25],[26],[27].

In IES, the dynamic cybersecurity model can be complemented or integrated into their Information Security Management System.

This dynamic cybersecurity model can be easily adapted to the processes, procedures and / or dependencies of each IES.

It is important that the instrument to assess the cybersecurity model meets the levels of reliability, validity, and objectivity.

To apply the dynamic cybersecurity model in an IES, the legal provisions and standards that frame the procedures in the institution must be identified.

The instrument must be validated by the expert personnel responsible for the procedures of the model in the institution.

5. REFERENCES

[1] F. Carrera Villacrés, L. Vernaza Quiñónez, F. Quiroz Ponce, K. Solís Charcopa, and E. Vicente da Silva, "Cybersecurity in the information systems of universities," *Science Domain*, vol. 3, no. 3, pp. 689–713, 2017. doi: 10.23857 / dc.v3i3.

[2] C.C. Police, "Colombia Cybercrime Trends 2019-2020," 2019.

[3] R. Sabillón, J.J.C.M., "Audits in Cybersecurity: A model of general application for companies and nations," *RISTI - Rev. Ibérica Sist. e Tecnol. Information*, no. 32, pp. 33–48, 2019. doi: 10.17013 / risti.32.33-48.

[4] J.J. Santacruz Espinoza, C.R. Vega Abad, L.F. Pinos Castillo, O.E. Cárdenas Villavicencio, "Cobit system in computer systems auditing processes," vol. 2, no. 8, pp. 65–68, 2017.

[5] J. Morales, N. Zambrano, J. Mera, M. Zambrano, "Cybersecurity and its application in Higher Education Institutions," *RISTI - Rev. Iber. Syst. e Tecnol. Inf.*, pp. 438–448, 2019.

[6] S. Consulting, "Implementing the ISO 27032: 2012 Standard," 2019.

[7] B. José, R. Montealegre, "Measurement of Cybersecurity maturity in Colombian MSMEs," 2016.

[8] C. Tarazona, "Computer Threats and Information Security," *Information Security Consultant, Etek Internacional.* pp. 137–146, 2015.

[9] S. Ontoria, "Government and modeling of information security in organizations," Universidad Carlos III Madrid, 2011.

[10] A. Valoyes Mosquera, "Cybersecurity in Colombia," *Univ. Pilo*, p. 12, 2019.

[11] J. Burgos Salazar, P.G. Campos, "Model for information security in IT," *CEUR Workshop Proc.*, vol. 488, pp. 234–253, 2009.

[12] R. Hernández Sampieri, C.P. Mendoza Torres, "The Quantitative, Qualitative and Mixed Routes Research Methodology," *McGraw-Hill Interam.*, p. 713, 2018.

[13] SL Guzmán Solano, "Guide for the implementation of the ISO 27032 Standard," Universidad Catolica de Colombia, 2019.

[14] ICONTEC, *GTC-ISO / IEC 27032*. 2020, p. 69.

[15] ID Advisors, "Quick guide to ISO 20000-1: 2018 Service Management System application," 2018. [Online]. Available: https://www.intedya.com/productos/GUIAISO20000.pdf.

[16] J.S. Acosta, "Design of a security policy model for a server," Universidad Cooperativa de Colombia, 2018.

[17] AENOR, "Information Technology Security Techniques Code of Practice for Information Security Controls ISO 27002," pp. 1–118, 2015.

[18] AENOR, "ISO / IEC / IEEE 29119 The new international standard for software testing," 2014. [Online]. Available: https://in2test.lsi.uniovi.es/gt26/presentations/ISO29119-Presentacion-GT26-20140618.pdf.

[19] AENOR, "Information Technology Software Asset Management (SAM)," pp. 1–3, 2008.

[20] E. Cajibal, "Vulnerability and social resilience to floods derived from tropical cyclones in three municipalities of Veracruz. A study with high school teachers," no. October, p. 295, 2018.

[21] J. J. Palacios Rozo, H. E. Palacio Velásquez, R. González Silva, "Educación versus tecnología y su convergencia hacia la IA," *Revista vínculos*, vol. 15, no. 2, pp. 186–194, nov. 2018. https://doi.org/10.14483/2322939X.14114

[22] R. E. Valero Vargas, J. J. Palacios Rozo, y R. González Silva, "Tecnologías de la Información y la Comunicación y los Objetos Virtuales de Aprendizaje: un apoyo a la presencialidad," *Revista vínculos*, vol. 16, no. 1, pp. 82–91, jun. 2019. https://doi.org/10.14483/2322939X.15537

[23] M. J. Hernandez Mediná, C. C. Pinzón Hernández, D. O. Díaz López, J. C. Garcia Ruiz, y R. A. Pinto Rico, "Open source intelligence (OSINT) in a colombian context and sentiment análisis", *Revista vínculos*, vol. 15, no. 2, pp. 195–214, nov. 2018. https://doi.org/10.14483/2322939X.13504

[24] C. Ruiz, "Interinstitutional Program Doctorate in Education.," *J. Chem. Inf. Model.*, vol. 53, no. 9, pp. 1689-1699, 2017.

[25] J. C. Najar Pacheco, "Exposición del activo más valioso de la organización, la ´información´", *Visión Electrónica*, vol. 11, no. 1, pp. 107-115, 2017. https://doi.org/10.14483/22484728.12345

[26] C. H. Caicedo, A. Smida, "Intensidad informacional para la longitudinalidad asistencial en sistemas de salud," *Visión electrónica*, vol. 10, no. 1, pp. 83-95, jun. 2016. https://doi.org/10.14483/22484728.11612

[27] J. F. Herrera-Cubides, P. A. Gaona-García, C. E. Montenegro-Marín, S. Sánchez-Alonso, y D. Martin-Moncunill, "Abstraction of linked data's world," *Visión electrónica,* vol. 13, no. 1, pp. 57-74, feb. 2019. https://doi.org/10.14483/22484728.14397

[28] J. P. Ortiz Quevedo, R. Nuñez Uribe, "Percepciones docentes de las didácticas en el entorno virtual," *Conocimiento Global*, vol. 4, no. 1, pp. 67-78. 2019. [Online]. Available: https://conocimientoglobal.org/revista/index.php/cglobal/article/view/35

[29] F. Agredo Satizábal, "Impacto de las TIC en la competitividad empresarial soportada por un modelo de educación digital," *Enfoque Disciplinario*, vol. 4, no. 1, pp. 37-50. 2019. http://enfoquedisciplinario.org/revista/index.php/enfoque/article/view/20

[30] A. F. Castro Alfaro. "El coaching como puntos de fortalecimiento del profesionalismo del docente," *Enfoque Disciplinario*, vol. 2, no. 1, pp. 15-22. 2017. [Online]. Available: http://enfoquedisciplinario.org/revista/index.php/enfoque/article/view/14