



Comparative Analysis of Methodologies for the development of Computer Audits considering: Risk Analysis, Data Mining, Reference Frameworks and Standards and International Standards for Standardization

Análisis Comparativo de Metodologías para el desarrollo de Auditorías Informáticas considerando: Análisis de Riesgos, Minería de Datos, Marcos y Normas de Referencia y Normas Internacionales de Normalización

Patricia Jimbo-Santana¹ , Karen Cabrera-Pantoja¹ , Mónica Jimbo-Santana¹ 

¹ Universidad Central del Ecuador, Quito, Ecuador
prjimbo@uce.edu.ec, klcabrera@uce.edu.ec, djimbo@uce.edu.ec

(Received: 23 February 2022; accepted: 15 February 2023; Published online: 30 June 2023)

Abstract. The computer audits that are carried out in organizations with or without profit, public or private, must use an adequate methodology and according to their objectives to solve the different problems that arise. For this reason, in this work comparisons are made between the methodologies for Risk Analysis, Data Mining, Reference Frameworks - Standards and International Standardization Norms, with the purpose of obtaining results and specific cases that allow the selection of an appropriate methodology against the problem to be solved in the organizations, or against what the organization wants to obtain as a result. All that, through the help of techniques or quantitative and qualitative comparison methods, established in the second part of the investigation; this will depend on which methodology can stand out against another. In the comparative tables, general and specific characteristics were analyzed, finding in the first part, the affinity that the methodologies have compared to their general phases and, when analyzing the specific characteristics, information was obtained that allowed each methodology to be distinguished and, in this way, find the distinctive results for each methodology.

Keywords: Computer Auditing, Computer Auditing Methodology, Risk Analysis, Data Mining, Reference Frames, ISO standards.

Resumen. Las auditorías informáticas que se realizan en organizaciones con o sin ánimo de lucro, públicas o privadas, deben utilizar una metodología adecuada y acorde a sus objetivos para resolver los diferentes problemas que se plantean. Por ello, en este trabajo se realizan comparaciones entre las metodologías de Análisis de Riesgos Análisis, Minería de Datos, Marcos de Referencia - Estándares y Normas Internacionales de Normalización, con el fin de obtener resultados y casos concretos que permitan la selección de una adecuada metodología adecuada frente al problema a resolver en las organizaciones, o frente a lo que la organización desea obtener como resultado. Todo ello, mediante la ayuda de técnicas o métodos de comparación cuantitativos y cualitativos métodos de comparación, establecidos en la segunda parte de la investigación; de ello dependerá que metodología puede destacar frente a otra. En los cuadros comparativos se analizaron las se analizaron las características generales y específicas, encontrando en la primera parte, la afinidad que tienen las metodologías en comparación con sus fases generales y, al analizar las características específicas, se obtuvo información información que permitió distinguir cada metodología y, de esta manera, encontrar los resultados resultados de cada metodología.

Palabras clave: Auditoría informática, Metodología de auditoría informática, Análisis de riesgos, Minería de datos, Marcos de referencia, Normas ISO.

Paper Type: Research Paper.

1 Introduction

The need to have control of information has grown over time, even more so when we find ourselves in an era of technological revolution where information has become the most important asset of different

organizations. This is why it is necessary to measure, safeguard, secure, analyze information as an essential part of companies, whether they are public, private, for-profit, or non-profit, taking force to carry out a computer audit. This audit is used to evaluate in depth the computer and technological resources that an entity has, and there are many methodologies that, over time, have evolved in order to obtain efficiency and effectiveness in the processes and activities that are carried out, and where the aforementioned elements intervene.

Currently, having a wide variety of methodologies that allow computer audits, it is essential to form a classification that generalizes those methodologies that pursue the same purpose. Therefore, the methodologies focused on Risk Analysis, Data Mining, Reference Frameworks and Standards, and International Standardization Norms are presented, explaining in each of them definitions, structure, phases, content, versions, and other information of useful aid that will serve to define them clearly.

It is important to compare the methodologies, since in each of their classifications it is imperative to clarify everything that a comparative method entails: definitions and techniques that allow finding similarities, inequalities or additional utilities that open the way to obtaining specifications that help organizations to find the most appropriate methodology. In each methodology the same goal is followed; however, each returns different results. This characteristic is what will allow the selection of the methodology, since it will depend on the problem that arises in a specific case study in organizations, which becomes the objective of this scientific article.

2 Computer audit methodologies

A classification is made among the existing methodologies in: Risk analysis, Data mining, Reference frameworks and standards, and international norms of standardization.

2.1 Risk analysis

According to the International Organization for Standardization (ISO), "a risk is the probability that a given threat will materialize by exploiting the vulnerabilities of an asset or group of assets and therefore cause damage or loss to the organization" (Arévalo *et al.*, 2017). For this reason, there are methodologies that propose not only to identify the possible risks that can occur within an organization, but also to establish measures that are considered as contingency plans to avoid the different risks identified. In this way, information assets are protected, threats are avoided, vulnerabilities are corrected, and the impact is reduced.

In this methodology there are also quantitative and qualitative approaches, directing their choice, above all, to the quantitative approach. According to Eterovic & Pagliari (2011), this last approach "consists in obtaining a value from the product of these elements. The way to calculate it, for a given event, is by multiplying the value of the potential loss by the value of the probability of occurrence", so the application form is simpler to assess the different risks by calculating the probability that these have, reducing the relevance of qualitative analysis as it is a "subjective choice".

In the risk analysis methodologies, there are other methodologies that are used to define findings in a different way. These are:

- **MAGERIT**. It consists of analyzing, through a series of steps that, according to García and Moreta (2019), are: "Determination of relevant assets, determination of threats, determination of safeguards, impact estimation and risk estimation", the correct use of technologies of information to identify possible risks and, thanks to this, to be able to implement security measures that allow the previously identified risks to be reduced and probably entrenched (Horvey, S. *et al.*, 2023).
- **OCTAVE**. It focuses on the analysis of the risks of organizations. According to Guanoluisa & Maldonado (2015), OCTAVE methodology covers "from a team of people from the operational or business sector to one from the information technology (IT) department, thus managing to focus on security needs in three aspects: Risks Operations, Security Practices and Technology". Therefore, this methodology not only considers the technology that the company has, but also the organizational risks that may arise.
- **MEHARI**. It is responsible for "supporting those responsible for a company's computer security through a rigorous analysis of the main risk factors, evaluating quantitatively, according to the

situation of the organization, where the analysis is required" (Alemán Novoa & Rodríguez Barrera, 2015), thus helping to manage all the activities carried out by the IT department.

- **NIST SP 800 – 30.** It is aimed at information security. According to the Organization of American States (2019), "the framework adopted as a strategy to base itself on industry standards already accepted by the cybersecurity ecosystem (NIST SP 800-53, ISO/IEC 27001:2013, COBIT 5, CIS CSC, among others)". This allowed expanding and improving data security protection, making NIST SP the best option when disaster planning and recovery is required in information technology domains.
- **CORAS.** It is a platform used for the evaluation of critical risks of the information technology department. CORAS is supported by a Unified Modeling Language (UML), which corresponds to a practical language that aims to unify the system to be built in its development. This methodology, according to López (2018), contains phases, elements, and support methods that "with the complementary support of the methods, increases the confidentiality, integrity, availability and responsibility of the application, encompassing the appropriate potential threats and covering all the phases of the process."
- **CRAMM.** Risk analysis methodology developed by the Central Agency for Communication and Telecommunications (CCTA); this factor makes CRAMM the most widely used methodology in organizations in Europe. The objective of this methodology is to adhere to the principles of confidentiality, security, integrity, protection, and availability of information systems. Its structure, according to Cordero (2015), is phases, elements, processes that "in the first stage aspires to collect the global definition of security objectives. In the second stage, it identifies the risks through materialization; and, in its last stage, it identifies and selects the security measures that must be applied in the organization."
- **OSSTMM.** According to Miranda Silva (2019), OSSTMM is a "methodology that proposes a process for assessing weaknesses in a series of areas that faithfully reflects the levels of security present in the infrastructure that is going to be audited." In other words, the objective of this methodology is to strengthen the weak areas in the security aspect of the component to be audited. The OSSTMM methodology began as a manual of good practices, but, in view of its enormous reception, it became a guide for auditing; for this reason, the phases presented contemplate a specific and summarized guide to the process of applying an audit.
- **EBIOS.** It aims to ensure that the security objectives and requirements are aligned with the system under study, considering the business processes involved, and in turn, its five phases which, according to Alemán and Rodríguez (2015), are: "Study of the context, Study of the dangerous elements, Study of the threat scenarios, Study of the risks, Study of the security measures". This allows it to become a tool that allows the company to build a repository for Information Security Systems, thereby helping to manage risks by developing a strategy to carry out its implementation.

Once each of the risk analysis methodologies has been defined, [Table 1](#) is established, which presents the cases of use of each methodology to group the problems that may occur in a company and thus choose the methodology that associate.

Table 1. Comparison of specific characteristics of Risk Analysis Methodologies.

Risk analysis methodologies	Area of application	Phases	Use cases
MAGERIT	Government, Organisms, Big companies, SME, Commercial and not commercial companies.	<ol style="list-style-type: none"> 1. Determination of relevant assets. 2. Threat determination. 3. Determination of Safeguards. 4. Impact Estimate. 5. Risk Estimate. 	When it's requested: <ul style="list-style-type: none"> • A study of the files affected by the legislation on personal data, of the guarantees of confidentiality of the information, of the security of communications and perimeter, of the availability of services. • In addition to a homologation or accreditation of the system or a product, or when seeking to launch a security metrics project, identifying which points are of interest to

Risk analysis methodologies	Area of application	Phases	Use cases
			control and with what degree of frequency and detail. At the same time: <ul style="list-style-type: none"> • Urgent analysis to determine critical assets. • Global analysis to determine general measures. • Detailed analysis to determine specific safeguards for certain elements of the information system or quantitative detail to determine the opportunity of a high expense.
OCTAVE	Applicable for small and large companies, each with its specific version.	<ol style="list-style-type: none"> 1. Vision of the organization. 2. Technological Vision. 3. Planning of measures and risk reduction. 	When the company faces the following scenarios of threats to information assets: <ul style="list-style-type: none"> • Accidentally or directly, attacking the organization's technical infrastructure. • By physical access directly or on its container, whether accidental or deliberate to the organization. • For problems with the organization's technology and information systems (hardware, software, viruses, and other system-related problems).
MEHARI	Government, Organisms, Medium and Big companies, Commercial companies, without profit (education, health services public, non-governmental organizations).	<ol style="list-style-type: none"> 1. Risk assessment. 2. Risk treatment. 3. Risk management. 	When the company needs to obtain: <ul style="list-style-type: none"> • Control category levels. • Quality levels of security services • The evaluation of the quality of the service by means of questionnaires. • A model table of impacts.
NIST SP 800:30	Used by governmental and non-governmental organizations.	<ol style="list-style-type: none"> 1. Characterization of systems. 2. Threat identification. 3. Identification of vulnerabilities. 4. Analysis of controls. 5. Determination of probabilities. 6. Impact analysis. 7. Risk determination. 8. Recommendation of controls. 	When the company is facing: <ul style="list-style-type: none"> • Vandalism. • Leakage of internal information, Hacking, Theft. • Infrastructural threats. • Internet service failures, computer services, or malfunction of internal applications. • Absence of contingency plans • Damage to the organization's facilities that could affect the hardware or software.
CORAS	Applicable for public or private sector companies.	<ol style="list-style-type: none"> 1. Context identification. 2. Identification and risks. 3. Risk analysis. 4. Risk assessment. 5. Treatment of risks. 	On: <ul style="list-style-type: none"> • Detection of security flaws. • Inconsistencies. • Redundancy. • Discovery of security vulnerabilities.

Risk analysis methodologies	Area of application	Phases	Use cases
CRAMM	Public and private organizations.	<ol style="list-style-type: none"> 1. Establishment of security objectives. 2. Risk assessment. 3. Identification and selection of countermeasures. 	When the company requires: <ul style="list-style-type: none"> • A high-level risk analysis that is necessary to identify the general or emergency security requirements for the organization, the relative costs, and the implications of their implementation. • Identify the general security requirements, contingency and associated costs of the various options when conducting the feasibility study. • A pre-execution review to ensure that all physical, personnel, technical, and security countermeasures have been identified and implemented.
OSSTMM	Public and private organizations.	<ol style="list-style-type: none"> 1. Induction. 2. Interaction. 3. Research. 4. Intervention. 	When the organization needs: <ul style="list-style-type: none"> • Cloud computing test. • Virtual infrastructures. • Messaging middleware. • Mobile communication infrastructures. • High security locations. • Plan the project, quantify results, and the rules of the contract to perform security audits.
EBIOS	Mostly used by the Public Sector but can also be applied in the private sector.	<ol style="list-style-type: none"> 1. Study of the context. 2. Study of dangerous elements. 3. Study of threat scenarios. 4. Study of the risks. 5. Study of security measures. 	When: <ul style="list-style-type: none"> • There is the possibility of covert functions introduced during the design or development phase (software), or the use of untested hardware (hardware). • There is the possibility of creating or modifying system commands (networks), or the establishment can be penetrated through indirect access (local), appearing non-compliance with instructions by some operators (staff). • There is a lack of security measures in the design, commissioning, and management phases.

According to what is analyzed in [Table 1](#), we can indicate that:

- All the methodologies in their field of application can be used in organizations, both public and private, but it is the characteristics that they present that distinguish them.
- The CORAS and MEHARI methodologies are the only ones that, in addition to being considered as methodologies as such, are also considered as support tools that can be used in any part of the project.
- It is only the CORAS methodology that performs a qualitative analysis since the other methodologies can be presented both qualitatively and quantitatively.
- In the research carried out, the authors of the different bibliographic bases (Alemán & Rodríguez, 2015; García & Moreta, 2019; Guanoluiza & Maldonado, 2015; López, 2018; Miranda, 2019), in the comparisons between different methodologies, emphasize the choice of MAGERIT as the main methodology to choose, since as a result a list of critical assets is obtained where organizations can verify the assets that should be approached more objectively.

- In turn, OSSTMM is one of the methodologies that allow the most tests to be carried out to find the vulnerabilities and risks that may arise, since it includes both physical and technological tests.
- Although each methodology has its scope of application because some organizations use them more than others, they can all be applied to private, public, for-profit or non-profit companies.

The purpose of the methodologies of this classification will always be to mitigate the risks encountered through contingency plans that can be tested and improved. However, it is the use that will determine the difference.

2.2 Data mining

The methodologies for the analysis of data mining exist to find patterns that, through the help of statistical tools, influence decision-making and generate a change or improvement within it. Generally, this methodology uses algorithms that allow obtaining quantitative results through the application of the phases of the methodologies; however, it contemplates an established general process that is made up of, according to Gallardo (2016), the preparation of the data, selection of tools and initial modeling, refinement of the selected model, implementation of the model and the communication of results, which makes it in a useful methodology for the processing of abundant information. Within data mining, there are several applicants that allow adapting to the situation in which they find themselves, which are:

- **KDD.** According to Timarán et al. (2016), "the process consists of extracting patterns in the form of rules or functions, from the data, for the user to analyze them", combining analysis with discovery; hence its name, "Knowledge Discovery in Databases" originates. What this methodology intends is to automate the processes so that the people in charge carry out other activities with the remaining time, acting iteratively and interactively.
- **CRISP DM.** It is a methodology focused on users, in this case business users, so that they can read in a more comprehensive way the data they have within their organization, where the success of the project to be applied will be measured through said compression. According to Galán (2015), the phases include business understanding, data understanding, data preparation, modeling, evaluation, and implementation.
- **CATALYST.** This methodology distinguishes two important models: the Business Model and the Information Exploitation Model, the latter also considered as data mining. According to Moine (2011), P3TQ relationships refer to having the right product, in the right place, at the right time, in the right quantity, and at the right price. This is how the study begins from the organizational value chain, which consists of supply processes, technological development, human resources, company infrastructure, internal logistics, operations, marketing and sales, external logistics and services.

It is also necessary to analyze the phases and fields of application that each methodology has, which is indicated in Table 2, where the use cases in which it can be used are specified:

Table 2. Comparison of specific characteristics of Data Mining Methodologies.

Data mining methodologies	Area of application	Phases	Use cases
KDD	Applicable for companies and companies that handle large public and private databases.	<ol style="list-style-type: none"> 1. Problem identification. 2. Selection. 3. Pre-processing. 4. Transformation/reduction. 5. Data mining. 6. Interpretation/evaluation of data. 	<p>It is used when there are unknowns of large information data.</p> <p>In addition, it is used for the extraction of previously unknown knowledge.</p> <p>It is also used for predicting data based on patterns.</p>

Data mining methodologies	Area of application	Phases	Use cases
CRISP DM	Applicable for commercial, government and academic companies.	<ol style="list-style-type: none"> 1. Business understanding. 2. Understanding the data. 3. Data preparation. 4. Modeling. 5. Evaluation. 6. Implementation. 	<p>It is used based on a set of tasks having hierarchy.</p> <p>It is used to apply in projects for more reliable predictions, from the established data.</p>
CATALYST	Applicable for for-profit or non-profit organizations.	<ol style="list-style-type: none"> 1. Data preparation. 2. Selection of tools and initial modeling. 3. Refine the model. 4. Implement the model. 	<p>Applies to business models.</p> <p>It does not work directly with the data, but with the needs of the client.</p> <p>It is based on patterns according to the identified business problem.</p>

According to what is indicated in Table 2, the following results are obtained:

- CRISP DM and CATALYST are noted to provide insights through data collection, use, and management.
- All the methodologies described are based on data that result in the use of patterns and relationships that exist between collected data and analyzed data.
- The data analysis of the methodologies provides support for the generation of business intelligence, and this allows organizations to have foundations for correct and timely decision making.
- Currently, the most used methodology for data mining is CRISP DM, since it manages all the information for a better work in different projects based on customer profiles.
- Each of the methodologies, to be applied, is supported by computer tools such as free software to obtain results. There are a number of programs intended to be the support of the methodologies or that were created at the beginning of the same, such as: RapidMiner, IBM SPSS, R, SAS, Python, Orange, Weka, Knime, being applicable to Windows, LinuxMacOS.

The purpose of comparing the cited methodologies is to provide a tool so that the work teams of the organizations can evaluate the data with the help of the pertinently chosen methodology. In other words, depending on the problem with the data, the methodology that tends to provide the appropriate solution will be chosen.

2.3 Reference frameworks and standards

For carrying out computer audits, there are also reference frameworks known as good practices and standards, which are a guide of steps for the correct application of the processes. Good practices allow that, when companies apply them, their processes are adjusted to their needs, which will give access to the best management of the business area, considering several factors. But it is convenient to consider the characteristics that good practices present in order to verify the place where it is applied.

The environment of good practices, according to Valverde et al. (2016), represent a complete panorama of the aspects that a good practice takes into account, that is, it can be applied in different entities and its purpose is to direct a process, become a technique that allows to fulfill the aforementioned objectives and, at the same time, uniting all this environment is formalized in manual, code, protocol, among others. They also want to improve all the processes that the organization has, including internal communication to spread the improvements obtained in the most appropriate way. Therefore, a good practice will be considered as an agent of change that, when applied, will help in the audit process. Within the best known and referenced best practices or reference frameworks, there are:

- **ITIL V4.** It is based on a set of good practices for the use of information technologies, apart from the life cycle of the IT service, made up of strategy, design, transition, operation, and continuous improvement of the service. They appear, according to Berger et al. (2020), other applicants that

may have greater flexibility in their processes, implementing the components of Basic principles, Governance, Service value chain, Practices, Continuous improvement. Having in turn 34 practices, which are divided into three sections: general, service and techniques.

- **COSO IV.** This framework is based on five components and seventeen principles that relate to the organization's objectives: operational, information and compliance. The purpose of this framework is to design, implement, evaluate, and improve internal control in organizations. Internal control is the set of measures and procedures that an organization establishes to ensure the achievement of its objectives, the protection of its assets, the reliability of its information and the efficiency of its operations (Dvorski Lacković, et al., 2021).
- **COBIT 2019.** It is a guide to good practices, also considered a reference framework, with the mission of controlling and supervising information technology control activities (Fernandes et al., 2020). It presents an approach that optimizes IT governance, since according to ISACA (2012), it helps IT professionals and organization leaders to carry out their responsibilities in IT management and governance, particularly in the areas of assurance, security, risk and control and provide value to the business (De Haes, et al., 2019). It changes the limitations found in its previous version, COBIT 5, but maintains its bases: Realization of benefits, optimization of risks and resources.

The specific characteristics of the Reference Frameworks and Standards are presented to identify their scope of application, phases and use cases in [Table 3](#):

Table 3. Comparison of specific characteristics of Data Mining Methodologies.

Reference frameworks and standards methodologies	Area of application	Phases	Use cases
COSO IV	Companies, organizations, and public entities. It can also be adapted to different levels of the organization, from the corporate level to the operational level, through the business or functional level.	<ol style="list-style-type: none"> 1. Five component. 2. Seventeen principles 3. Phases: <ul style="list-style-type: none"> • Governance and culture. • Strategy and objective setting. • Performance. 	<p>It groups corporate policies, human resources procedures and operating mechanisms.</p> <p>When the company needs to obtain internal and external reports, both financial and non-financial Align risk with strategy. Improve risk-based decision making. Reduce operational surprises and losses, identify, and manage interrelated risks, leverage opportunities, and enhance growth and innovation in the organization.</p>
COBIT 2019	Organizations and companies.	<ol style="list-style-type: none"> 1. Understand the business context and strategy. 2. Determine the initial scope of the Government System. 3. Refine the scope of the Government System. 4. Conclude the design of the Government System. 	<p>It applies to information systems throughout the enterprise, including personal computers and networks.</p>

Reference frameworks and standards methodologies	Area of application	Phases	Use cases
ITIL V4	Organizations, public and private companies.	<ol style="list-style-type: none"> 1. Basic principles. 2. Governance. 3. Service value chain. 4. Practices. 5. Continuous improvement. 	<p>When you want to implement a new change management.</p> <p>When you want to improve the stability of the infrastructure.</p>

With the comparison in Table 3, it is obtained that:

- COBIT 2019 is an improvement for the limitations that COBIT 5 presented, therefore, by following the implementation phases, you will obtain an optimization, not only of the government but also of the Information Technology department, adapting to the needs of the organization.
- COBIT 2019 allows IT Governance to be a fundamental part of Corporate Governance, separating the management level (government) from the executive level (management) (Visitsilp B, et al., 2021).
- COSO IV aims to provide a framework for risk management and internal control that helps organizations achieve their goals and improve their performance (Santomil, P. et al., 2020). COSO IV seeks that organizations recognize and maximize the use of the supervision of their internal control systems when it is effective and increase the supervision in those areas that require improvement. It is based on five pillars: governance and culture, strategy and objective setting, performance, review and information, communication, and information.
- The ITIL V4 life cycle is represented in its previous versions, considering the strategy, design, transition, operation, and continuous improvement of the service. However, it is the new component of the service value chain that allows the new components to be introduced and the structure to be extended in such a way that a broader scope is obtained.

2.4 International Standardization Norms

The international standardization norms were created by the International Organization for Standardization (ISO), an entity constituted with the collaboration of several countries with the aim of creating applicable standards in different areas and guaranteeing that companies that have these standards obtain products and processes of quality. According to the ISO website (2021), there are countless Standards according to the scope of application, be they quality, environment, risks and safety, and social responsibility. However, in this research the ISO 27000 family will be emphasized, since according to Arias (2017), this standard has the following objectives: review and apply the continuous improvement of the ISMS, obtain evaluation metrics, document the treatment of risks, manage, control, and treat according to risks, identify, and assign responsibilities, generate evidence, and monitor risks.

- **ISO 27001 STANDARD.** Contains everything related to the requirements of a Security Management System. Valencia and Orozco (2017) point out that this standard "specifies the requirements for the establishment, implementation, operation, monitoring, review, maintenance and improvement of a duly formalized ISMS", its main objective being to provide feedback after its application by identifying the risks presented, considering access to accurate and complete information with immediate availability, without giving permission to unauthorized persons, thus complying with its principles of confidentiality, integrity and availability.
- **ISO 27002 STANDARD.** This standard was born because of the name change of the standard previously called ISO 17799, becoming part of the standards of the regulation in 1995 and following the directions established in ISO27001; that is, ISO27002 represents a complement to ISO27001.
- **ISO 27007 STANDARD.** It is a guide that helps organizations that are already certified to audit an Information Security Management System, using good practices to guarantee the confidentiality, integrity, and security of information, considering that the controls that mitigate

the risks are adequate, according to the problems presented, while the data in the information systems are true and related to the organization.

- **ISO 27017 STANDARD.** It is based on the 27002 standards, since it seeks to be a reference that helps to select the security controls that must be used when the information is in the cloud, specifying responsibilities and functions of the area. This makes ISO 27017 one of the most important standards for companies that handle this type of information, whether they are suppliers or clients, since it can be certified.
- **ISO 27032 STANDARD.** It is responsible for strengthening the company's cyber security, that is, guaranteeing security when information is exchanged on the network, improving Internet security, reducing the possibility that the organization's information is exposed to hackers, theft, alterations, virus exposures. (Sabillón, R. 2021).
- **ISO 38500 STANDARD.** It establishes guidelines for the Governance of Information Technology in organizations. According to (Robayo et al., 2020) it provides a framework for decision making related to IT, focusing on the alignment of IT with business objectives, risk management, compliance, and performance measurement. This standard is applicable to organizations of all sizes and sectors, and focuses on key roles and responsibilities, such as the board of directors and senior management, to ensure effective IT governance. Its objective is to improve the management and value of IT in support of the strategic objectives of the organization. (Rodríguez et al., 2019).

The comparative [Table 4](#) is established that will allow to clearly differentiate the specific characteristics that are presented:

Table 4. Comparison of specific characteristics of the International Standardization Norms.

International standardization norms	Area of application	Phases	Use cases
ISO 27001	Public and private companies and organizations	<ol style="list-style-type: none"> 1. Define the organization's security policy. 2. Define the scope of the ISMS. 3. Analyze the risks. 4. Manage risks. 5. Select controls. 6. Declare the applicability of controls. 7. Review the ISMS. 	<ul style="list-style-type: none"> • Used in risk analysis requirements. • When it is required to ensure the resources for the implementation of a system. • When documentation is required on the requested information. • When required to track performance and monitoring information. • When it is required to automate a system. • When it is required to make documented decisions on the treatment of risks.
ISO 27002	Public and private companies and organizations	<ol style="list-style-type: none"> 1. Define security policies. 2. Define the scope of the ISMS. 3. Analyze the risks. 4. Manage risks. 5. Select control targets. 6. Implement control objectives. 7. Certification. 	<ul style="list-style-type: none"> • For security policies. • For network communication management. • Uses a catalog of practices. • When sensitive or critical information is being processed. • When required to make a checklist for the implementation of new policies. • When you want to describe the departments, areas or activities of a company that are affected by the policy.

International standardization norms	Area of application	Phases	Use cases
ISO 27007	Company and organizations.	The phases that ISO 27007 handles are from ISO 27001 and 27002.	<ul style="list-style-type: none"> • It is used when management is required based on an ISMS audit program. • When auditing is desired, manage audit risks and thus assign appropriate auditors. When it is required to maintain the records that the company presents.
ISO 27017	Technology companies.	<ol style="list-style-type: none"> 1. Define security policies. 2. Define the scope of the ISMS. 3. Analyze the risks. 4. Manage risks. 5. Select control targets. 6. Implement control objectives. 7. Certification. 	<ul style="list-style-type: none"> • Used to standardize relationships between customers and cloud service providers. • When assets are required to be removed or returned when a contract is terminated. • It is used for the protection and separation of the client's virtual environment. • When a configuration of a virtual machine is required. • When it is required to track customer activity in the cloud. • When it is required to resolve an alignment of the virtual network and cloud environment.
ISO 27032	Company and cybersecurity organizations.	<ol style="list-style-type: none"> 1. Organization. 2. Risk analysis. 3. Action plan. 4. Implementation. 	<ul style="list-style-type: none"> • Used during exchanges, to avoid hacking, sabotage or alterations that could put it at risk. • When it is required to make a change of technologies in which it can be implemented. • When there is a change of security tools. • When you want to implement security of digital assets. • It is used in risk management.
ISO 38500	Company and organizations.	<ol style="list-style-type: none"> 1. Evaluation of IT Governance. 2. Implementation. 3. Review and monitoring. 	<ul style="list-style-type: none"> • Used to audit IT Governance. • Establishment of IT Governance. • Evaluation of IT Governance. • Improvement of IT Governance. • Alignment of IT with business strategy. • IT risk management. • Strategic decision making on IT. • IT project management. • IT governance culture. • Information security management.

According to what is obtained in [Table 4](#), it should be clarified that, of all the standards, ISO 27002 is the only one considered as a manual for good practices, which is why it uses a catalog of practices aimed at security policies that are going to be used in the organization. In the same way, the information must be considered sensitive or critical for this standard to be used.

The ISO 27007 standard contemplates the same application phases as the ISO27001 and 270002 standards. However, it is used when it is required to carry out management based on an ISMS audit program.

On the contrary, the ISO27017 standard presents a different vision, since it focuses its attention on the relationship between the client and the provider in the cloud, serving as an intermediary when problems arise between them.

On the other hand, the 27032 standard is considered as a standard focused on organizations that wish to avoid sabotage when information is exchanged when buying and selling products.

We can indicate that ISO/IEC 38500 is applicable in a wide variety of contexts related to IT governance and is used to establish, evaluate, and improve IT governance practices in an organization.

3 Results

When companies apply any of the methodologies indicated above, they will obtain different results, aimed at solving a specific problem. Therefore, it is important to define what result can be obtained when choosing a particular methodology. Each organization presents different difficulties, so in Table 5, each of the methodologies is summarized against its result to adapt to a specific need.

Table 5. Results obtained against computer audit methodologies based on: Risk Analysis, Data Mining, Reference Frameworks and Standards and International Standardization norms.

Methodologies	Results obtained
Risk analysis	
MAGERIT	<ul style="list-style-type: none"> - Measurement of the vulnerability of the threat. - Personal, confidential, information security, communication and services files completely studied and reviewed. - Approved products or systems. - List of critical assets. - List of general measures for critical assets. - Low-cost but effective safeguards. Risks of: <ul style="list-style-type: none"> • Unauthorized access. • Data loss. • Service interruption. • Malware and viruses. • Social engineering. • Insecure software development. • Advanced cyberattacks. • Identity and access management.
OCTAVE	<ul style="list-style-type: none"> - Risk mitigation plans, short-term action items to address specific weaknesses. - List of information assets that follow the mission of the organization. - List of the results that follow the line of good security practices. - A risk profile for each asset recognized as a critical asset. Risks of: <ul style="list-style-type: none"> • Business interruption. • Unauthorized access. • Data loss. • Software vulnerabilities. • Malware and viruses. • Governance and management. • Business continuity.
MEHARI	<ul style="list-style-type: none"> - Expresses security threats, resulting in the scale of malfunction values and the classification of information and assets. - Categorized security controls. - High-end security services. - Questionnaires that evaluate the quality of the service. - IT impacts with recurring risks shown in tables. Risks of: <ul style="list-style-type: none"> • Unauthorized access. • Information leakage. • Malware and viruses. • Identity and access management. • Software vulnerabilities.

Methodologies	Results obtained
	<ul style="list-style-type: none"> • Insufficient security controls. • Incident management. • Social engineering.
NIST SP 800:30	<p>Through the help of the documentation requested at the beginning of the application, the summary of the infrastructure, the identification of human threats, techniques, vulnerabilities, allows a plan to be obtained as a result for the treatment of all the risks identified in the previous information with a matrix establishing the suggested control and the level of risk impact.</p> <p>Risks of:</p> <ul style="list-style-type: none"> • Unauthorized access. • Software vulnerabilities. • Data leakage. • Disasters and business continuity. • Insufficient security controls. • Identity and access management. • Incident management.
CORAS	<p>The company detects, after its application, security vulnerabilities in a faster and more efficient way since, by managing language models based on Microsoft Visio, it obtains: an extensive list of cases that can be reusable, case management and a format widespread for reporting.</p> <p>Risks of:</p> <ul style="list-style-type: none"> • Unauthorized access. • Data loss. • Software vulnerabilities. • Information leaks. • Disasters and business continuity. • Inadequate security controls. • Security governance.
CRAMM	<p>By performing the risk analysis in a quantitative and qualitative way, it is possible to obtain as a result a list of general security and emergency requirements intertwined with low costs that allow their applicability, as well as a clear vision of the threats that can affect the business.</p> <p>Risks of:</p> <ul style="list-style-type: none"> • Unauthorized access. • Software vulnerabilities. • Data loss. • Disasters and business continuity. • Inadequate security controls. • Social engineering. • Incident management.
OSSTMM	<p>Quantified projects are obtained to establish security audits, in addition to tests in the cloud that discover problems in the flow of information. When performing the other established tests, findings are found that serve as a guide for the auditor. In turn, metrics that measure the performance of the areas to which it is applied.</p> <p>Risks of:</p> <ul style="list-style-type: none"> • Unauthorized access. • Software vulnerabilities. • Social engineering. • Malware and viruses. • Penetration testing. • Insecure software development. • Incorrect configuration. • Security governance. • Network security.
EBIOS	<p>Discover the hidden phases in the software or hardware that threaten the security of the information and that there are no changes in the system. In the same way, its results allow concrete descriptions, valuable challenges, clearly define the risks together with the detailed impact that it would cause to the organization, explicit security objectives and requirements for decision making.</p> <p>Risks of:</p> <ul style="list-style-type: none"> • Unauthorized access. • Information leaks. • Software vulnerabilities.

Methodologies	Results obtained
	<ul style="list-style-type: none"> • Malware and viruses. • Penetration testing. • Security governance. • Disaster and business continuity.
Data mining	
KDD	<p>After applying data processing and transformation, patterns are obtained with specific, consistent, and categorized data that allow decisions to be made. It can be useful in risk management for:</p> <ul style="list-style-type: none"> • Detecting risk patterns. • Predicting future risks. • Risk segmentation. • Resource optimization. • Improving decision-making. • Continuous risk monitoring.
CRISP DM	<p>It is applied to the analysis of a large amount of data, using software, it allows the development of models that can be used in business, to obtain greater profitability, improve processes and even models that surpass traditional models, these being possible to apply in various areas such as credit, banks, accounting, financial education, business, among others. It doesn't specifically focus on risk management, but its systematic and structured approach to data analysis projects can assist organizations in identifying, mitigating, and controlling risks associated with data mining and data-driven decision-making. By following the phases and best practices of CRISP-DM, organizations can enhance the quality of their data analyses and reduce potential risks associated with incorrect or biased data-driven decisions.</p>
CATALYST	<p>The Business Model is obtained to identify the business problem as such and the Data Mining Model that allows building "boxes" that determine the actions to be carried out after finding the findings. It plays a crucial role in safeguarding critical infrastructures and managing cyber risks in industrial control systems. It provides a framework and tools for identifying, assessing, and mitigating cyber risks in operational technology environments, thereby enhancing the security of essential infrastructure, and reducing exposure to cyber threats.</p>
Frameworks and standards	
COSO IV	<p>It helps organizations manage their risks strategically and in alignment with their objectives. It identifies and manages risk across the entire company, considering both internal and external factors that can impact its performance. It enhances positive outcomes and reduces negative surprises by anticipating potential threats and opportunities that may arise in the environment. It broadens the spectrum of opportunities for the organization by fostering a culture of innovation and continuous improvement that leverages available resources. It enhances resource allocation and boosts business resilience by optimizing the use of assets, human capital, and technology to create value. It reduces performance variability by establishing indicators and control mechanisms that enable the evaluation and improvement of risk management.</p>
COBIT 2019	<p>It focuses on the measurement of processes, through the application of metrics, RACI matrices and different tools established by the ISACA guide, allowing the identification of shortcomings throughout the application, whether they are found in the governance or management domains. It is fundamental for risk analysis because it provides a robust IT governance framework that intrinsically integrates risk management into the management and operation of information technology. This framework not only helps organizations identify and assess technology-related risks but also facilitates the implementation of effective controls and continuous risk monitoring. By aligning IT governance with strategic and business objectives, COBIT 2019 contributes to informed decision-making, improved operational efficiency, and adaptability in an ever-changing business environment, providing a comprehensive and balanced view of technology-related risks and opportunities.</p>
ITIL V4	<p>Like COBIT 2019, ITIL V4 analyzes the areas included through the value chain in the strategic areas, forming a matrix in each area as a model for both governance and management to improve these areas. It is essential for risk analysis in the context of IT service management because it provides a robust framework for service delivery and continuous improvement. By addressing service management from a holistic perspective, ITIL 4 enables organizations to identify and assess risks more effectively, especially in the delivery of critical services. Furthermore, it facilitates the integration of risk management best practices at all stages of the service lifecycle, from strategy to operation, thereby enhancing the organization's resilience, efficiency, and adaptability in the face of constantly evolving technological and business challenges.</p>

Methodologies	Results obtained
International standardization norms	
ISO 27001	Secure resources: automate information while a system is implemented. Helps decision-making for risk treatment. As a result of its application, a certification in Information Security Management Systems is obtained. It allows for the establishment of a strong and structured framework to identify and assess information security risks, leading to the implementation of effective controls. This strengthens the security of information assets and reduces exposure to cyber threats. Furthermore, by adhering to ISO 27001, transparency and trust are promoted, which can be crucial for gaining and maintaining the trust of customers and business partners. Finally, by proactively addressing information security, the organization can reduce the risk of costly and damaging security breaches while demonstrating its commitment to data protection and compliance with regulations, resulting in a competitive advantage in a digitally connected and highly regulated world.
ISO 27002	Obtains an analysis of security policies when applied, as well as a catalog of practices, obtaining a Guide to good practices of Information technologies to execute the Security Management System. It establishes a clear set of information security controls and best practices, facilitating the identification and rectification of vulnerabilities in IT systems and processes. Furthermore, by adhering to ISO 27002, the organization enhances its ability to safeguard critical information assets, reduce the risk of security breaches, and ensure the confidentiality, integrity, and availability of data. It can also assist in preparing to comply with data security regulations and standards, which is crucial in an increasingly regulated business environment. Ultimately, the adoption of ISO 27002 reinforces the confidence of customers and partners by demonstrating a strong commitment to information security and effective cyber risk management.
ISO 27007	It allows the selection of suitable auditors to carry out the management of the audit program, which will allow obtaining the correct administration of the risks and with this, the certification for good practices in terms of Security among clients. By following this standard, the organization can establish a robust framework for planning, conducting, and managing information security audits more effectively and efficiently. This includes risk identification, control assessment, policy and regulatory compliance reviews, and the identification of areas for improvement. Additionally, ISO 27007 promotes standardization and continuous improvement of audit practices, which can lead to greater confidence in the integrity of information security systems and processes and an increased ability to address cyber risks and meet security requirements.
ISO 27017	Standardization of the treatment between clients and providers in cloud systems, strengthening trust between users to obtain the certification to Adopt Security Measures for the Provision of Services in the cloud. This standard provides specific guidelines for cloud security, enabling the organization to identify and address risks associated with the adoption of cloud services more effectively. By adhering to ISO 27017, the organization can strengthen the protection of data and systems hosted in the cloud, ensure the confidentiality and integrity of information, and comply with applicable security regulations and standards. Furthermore, by demonstrating a strong focus on cloud security through ISO 27017-based audits, the organization can increase the confidence of customers and users in its information security practices in cloud environments, which can be crucial today in an increasingly cloud-dependent world.
ISO 27032	Changes of highly effective cloud security tools, as well as the protection of digital assets, avoiding hacks, sabotage of information. Therefore, a change in technologies is obtained as a result that allows a better development of online activities and the certification for the Manager considered as a Leader in Cybersecurity. This standard provides specific guidelines for managing information security in an increasingly digitally connected world, addressing cyber threats, and safeguarding critical assets. By adhering to ISO 27032, the organization can strengthen cyber resilience, identify, and effectively respond to cyber security incidents, and establish robust security governance across the enterprise. Furthermore, by demonstrating its commitment to cybersecurity through ISO 27032-based audits, the organization can build trust both internally and with its partners and customers, at a time when cyber security is crucial for business continuity and reputation.
ISO 38500	This standard establishes principles and guidelines for effective decision-making related to IT, including the management of cyber risks and systems auditing. By adhering to ISO 38500, the organization can ensure that its IT resources are used effectively to achieve strategic objectives and mitigate technology-related risks. Furthermore, by demonstrating a robust IT governance framework through ISO 38500-based audits, the organization can enhance transparency, accountability, and trust both internally and with external stakeholders, contributing to a stronger and more effective management of information technology.

Table 5 shows the results that any type of organization can obtain when applying a methodology to carry out a computer audit; everything will depend on the needs that organizations have in the face of the possible risks they face. It is important to emphasize that each methodology follows a different process, but they all have the same purpose. For this reason, it is possible to choose a methodology, not because its version is the most current or because it is the most selected, but because it adheres to the problem presented by an institution.

The results obtained from the analysis of the different methodologies indicate that:

- With risk analysis methodologies, highly secure systems are obtained that completely prevent the possibility of something happening or affecting the flow of information being handled. MAGERIT, OCTAVE and MEHARI are methodologies that provide a list of assets considered critical and important that must be protected to avoid any type of risk.
- CRAMM, on the contrary, issues a list of the general security and emergency requirements that counteract the identified vulnerabilities. NIST SP 800:30 and CORAS identify human, technical threats faster and more effectively using Microsoft Visio-based language.
- OSSTMM performs as many tests as possible through boxes that help identify information flow problems, like EBIOS, which discovers the hidden phases in the software or hardware that threaten information security.
- Although they are methodologies in which patterns are sought in the broad conglomerate of information, each one has its own process to follow. KDD becomes the methodology that begins the extraction of knowledge, so that with this management can make decisions.
- CRISP DM is the best-known methodology used by different authors when it is necessary to detect abnormal values. Its place gains strength internationally due to the field of application, since for the detection of said data, it considers the business from its compression to obtaining, according to that, the model for its implementation. This model can allow the formation of new processes in organizations, generating greater agility in them.
- CATALYST, for its part, considers the product, price, place, time, and quantity. Being so broad in its application, it also means more complexity, which is why CRISP DM continues to lead in use.
- COSO IV is an IT audit methodology that allows for the assessment and improvement of risk management and internal control within organizations, aligning them with their strategic objectives and performance. COSO IV is built upon five pillars that encompass all aspects relevant to the security and efficiency of information, from governance and culture to communication and data. COSO IV assists' organizations in identifying and managing risks that may impact their information, implementing appropriate control measures, monitoring their effectiveness, and ensuring compliance with applicable regulations and requirements. COSO IV also promotes a culture of innovation and continuous improvement that enhances the value and resilience of information.
- As mentioned above, the difference between COBIT 5 and COBIT 2019 focuses on the limitations of the previous guide. Currently, COBIT 2019 uses a process measurement model through CMMI (Capability Maturity Models), which will allow measuring the level at which a process is implemented and the way it performs, in addition to its design factors. that create a government system tailored to your needs.
- ITIL V4 maintains its initial structure; however, it no longer focuses only on service management, but, with the help of the value chain, allows a conjunction between the supplier and the client. Regardless of the additional guidance that ITIL includes, unlike its previous versions, it is the Service Value System that stands out as it covers all activities.
- Each of the standards has its certification, except for ISO 27002, which allows organizations to apply the standards in order to obtain a certification and that this is the added value that is delivered to the organizations, in view of the fact that complying with the protection of information has become an essential requirement that must be met.
- The benefits of obtaining certifications belonging to standards that are internationally recognized allow establishing a difference between competing companies in the same sector. For example, if a client wishes to choose a company to obtain his product, the company that has an international certification will have a higher profile and the client will be tempted to choose it.
- Over time, the use of technology has increased, and organizations have found it necessary to strengthen the security of the information they handle. The importance also lies in the fact that the

flow of information is increasing, so certification becomes a primary requirement to stand out in the market as an organization.

4 Conclusions and future work

From the description of the importance of the application of computer auditing for the identification of technological risks, it follows that information is the organization's most significant asset. Therefore, the resources, implements and assets that are immersed in this area must be inspected and evaluated to avoid any type of computer risk.

Based on the explanation of the existing computer audit methodologies, according to the established classification, it was possible to confirm that there are a large number of useful methodologies to perform computer audits, dating from the need to control the large amount of information that is handled. Given this, four general classifications are specified: i) Risk analysis, ii) Data mining, iii) Reference Frameworks and Standards and iv) International Standardization Norms, emphasizing the importance of each segmentation for choosing the appropriate methodology.

The development of IT audits requires methodologies that enable the assessment and improvement of the security, quality, and efficiency of an organization's information systems. Comparative analysis of these methodologies allows for the identification of their advantages and disadvantages, as well as their applicability and compatibility with the context and objectives of each audit. Thus, the most suitable methodology can be chosen for each case, resulting in reliable, valid, and useful outcomes for decision-making.

To carry out quantitative comparisons, there are clear and specific processes that allow obtaining defined results. However, for qualitative comparisons, it greatly infers the direction that the researcher gives to what he is doing; Therefore, there could be a certain bias when obtaining results. Despite the above, the techniques used by each of the comparisons exhibit a range of possible solutions to the problem at hand.

In the tables of specific comparisons of each classification of methodologies, the use cases were analyzed, which allowed defining the appropriate methodology against the need presented by the organization. With this previous analysis, it was determined that each methodology contains a different process, structure and elements that make each one have added value, even though they follow the same purpose. These characteristics allow breaking down particularities that help to solve problems and determine the methodology to select.

It is important to consider in future work, the review of case studies using the different methodologies in organizations, as well as proposing a theoretical model that explains the relationship between the factors influencing the selection and application of IT audit methodologies and their effects on achieving objectives and continuously improving information security and efficiency.

Statement of conflict of interest

The authors declared no potential conflicts of interest with respect to the research, authorship and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD

Patricia Jimbo Santana  <https://orcid.org/0000-0001-7432-1622>

Karen Cabrera Pantoja  <https://orcid.org/0000-0001-7598-0224>

Mónica Jimbo Santana  <https://orcid.org/0000-0002-3948-9507>

References

- Alemán, H. (2015). Metodología para la implementación de un SGSI en la fundación universitaria Juan de Castellanos, bajo la norma ISO 27001:2005. *Revista UNIR*. <https://www.unir.net/ingenieria/revista/auditoria-seguridad-informatica/>
- Alemán Novoa, H., & Rodríguez Barrera, C. (2015). Metodologías para el análisis de riesgos en los sgsi. *Publicaciones e Investigación*, 9, 73. <https://doi.org/10.22490/25394088.1435>
- Arias & Caycedo Casas, X. (2017). Auditoría informática: un enfoque efectivo. *Dominio de Las Ciencias*, 3, 157–173. <https://dialnet.unirioja.es/servlet/articulo?codigo=6102836>
- Arévalo, M., Cedillo, P., & Moscoso, S. (2017). Metodología Ágil para la Gestión de Riesgos Informáticos. *Revista Killkana Técnica*, 31–42. https://www.researchgate.net/publication/321176840_Metodologia_Agil_para_la_Gestion_de_Riesgos_Informaticos
- Berger, D., Shashidhar, N., & Varol, C. (2020). Using ITIL 4 in Security Management. *8th International Symposium on Digital Forensics and Security (ISDFS)*.
- De Haes, S., Van Grembergen, W., Joshi, A., & Huygh, T. (2019). COBIT as a Framework for Enterprise Governance of IT. *Management for Professionals*.
- Dvorski Lacković, I., Kurnoga, N., & Miloš Sprčić, D. (2021). Three-factor model of Enterprise Risk Management implementation: exploratory study of non-financial companies. *Risk Management*, 24, 101 - 122.
- Eterovic, E., & Pagliari, G. (2011). Metodología de Análisis de Riesgos Informáticos. *Dialnet*, 10. <https://dialnet.unirioja.es/servlet/articulo?codigo=3718552>
- Fernandes, A., Almeida, R. y Silva, MM (2020). Un método flexible para la selección de procesos COBIT 2019. *Conferencia de las Américas sobre Sistemas de Información*
- Galán Cortina, V. (2015). Aplicación de la Metodología Crisp-Dm a un Proyecto de Minería de Datos en el Entorno Universitario [Universidad Carlos III de Madrid Escuela Politécnica Superior]. https://e-archivo.uc3m.es/bitstream/handle/10016/22198/PFC_Victor_Galan_Cortina.pdf
- Gallardo, J. (n.d.). Los orígenes de CRISP-DM, se remontan hacia el año 1999 cuando un importante consorcio de empresas europeas tales como NCR (Dinamarca), AG(Alemania), SPSS (Inglaterra), OHRA (Holanda), Teradata, SPSS, y Daimler-Chrysler, proponen a partir de diferentes ver. *Sistemas Del Conocimiento*.
- García, F. Y. H., & Moreta, L. M. L. (2019). Modelo para Medir la Madurez del Análisis de Riesgo de los Activos de Información en el contexto de las Empresas Navieras. *RISTI - Revista Ibérica de Sistemas e Tecnologías de Informação*, 31, 1–17. <https://doi.org/10.17013/risti.31.1-17>
- Guanoluisa, J., & Maldonado, I. (2015). *ESCUELA POLITÉCNICA NACIONAL*. Quito: EPN, 2015. <http://bibdigital.epn.edu.ec/handle/15000/10499>
- Horvey, S.S., & Odei-Mensah, J. (2023). The measurements and performance of enterprise risk management: a comprehensive literature review. *Journal of Risk Research*, 26, 778 - 800.
- ISACA. (2012). COBIT 5: Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa. *ISACA PUBLICATIONS*. <https://www.isaca.org/>
- ISO. (2021). *ISO Tools*. <https://www.isotools.org/normas/>
- IsecT Ltd. (s. f.). ISO / IEC 27001 certification standard.
- León López, D. (2018). Implementación del Modelo COSO ERM 2017 en la Función Pública en Colombia. <https://reunir.unir.net/handle/123456789/7545>
- Lopez Ramirez, M. (2018). Análisis De Riesgos en un Sistema de Gestión de Seguridad de La Información (SGSI) con Metodologías Complementarias. *Universidad Piloto de Colombia*, 18.
- Miranda Silva, C. P. (2019). Auditoría de redes, aplicando la metodología OSSTMM V3, para el Ministerio de Inclusión Económica y Social. <https://repositorio.uta.edu.ec:8443/jspui/handle/123456789/30101>
- Moine, J. (2011). Estudio comparativo de metodologías para minería de datos. *Repositorio Institucional de La Universidad de La Plata*. https://repositoriosdigitales.mincyt.gob.ar/vufind/Record/SEDICI_5be4761a4607023df6968b1a4e548e7f
- Organización de los Estados Americanos. (2019). CIBERSEGURIDAD: MARCO NIST. *White Paper Series*. <https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf>
- Robayo Jácome, D. J., & Villarreal Morales, V. D. L. M. (2020). Convergencia de COBIT e ISO 38500 en el Gobierno de Tecnologías de la Información. <https://repositorio.uide.edu.ec/bitstream/37000/4152/1/1163-Texto%20del%20art%C3%ADculo-6196-1-10-20200507.pdf>
- Rodríguez, J., & Pérez, M. (2019). Análisis comparativo entre los modelos de gobierno y gestión de las tecnologías de la información COBIT 5 e ISO/IEC 38500:2015. *Revista Espacios*, 40(16), 17-28.
- Sabillón, R. (2021). Auditorías en Ciberseguridad. *Auditoría, garantía y concientización sobre seguridad cibernética a través de CSAM y CATRAM*.

- Santomil, P.D., & González, L.O. (2020). Enterprise risk management and Solvency II: the system of governance and the Own Risk and Solvency Assessment. *The Journal of Risk Finance*, 21, 317-332.
- Timarán, S., Hernández, I., Caicedo, S., Hidalgo, A., & Alvarado, J. (2016). Descubrimiento de patrones de desempeño académico. In *Descubrimiento de Patrones de Desempeño Académico* (Editorial, pp. 64–66). <http://dx.doi.org/10.16925/9789587600490>
- Valencia, F., & Orozco, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *Revista Ibérica de Sistemas y Tecnologías de Información*. <https://dialnet.unirioja.es/servlet/articulo?codigo=6672188>
- Valverde, J., Garrido, M., & Fernandez, R. (2016). Enseñar Y Aprender Con Tecnologías: un Modelo Teórico para las Buenas Prácticas Con TIC. *Teoría de La Educación. Educación y Cultura En La Sociedad de La Información*. <https://www.redalyc.org/pdf/2010/201014897009.pdf>
- Visitsilp B. and Bhumpenpein N, "Guidelines for Information Technology Governance Based on Integrated ISO 38500 and COBIT 2019, (2021) Research, Invention, and Innovation Congress: Innovation Electricals and Electronics (RI2C), Bangkok, Thailand, 2021, pp. 14-18, <http://dx.doi.org/10.1109/RI2C51727.2021.9559772>