UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Visión Electrónica
Más que un estado sólido
https://doi.org/10.14483/issn.2248-4728

VISIÓN ELECTRONICA
A case-study Vision

Implementation of cybersecurity risk analysis systems in Colombia

Implementación de sistemas de análisis de riesgos de ciberseguridad en Colombia

Felipe Andrés Corredor-Chavarro[1], Diana Cristina Franco-Mora[2], Diego Izquierdo-Dussan[3]

INFORMACIÓN DEL ARTICULO

Enviado: 30/11/2019
Recibido: 22/12/2019
Aceptado: 17/01/2020

Keywords:
ISO 27005,
Information security,
Risk management,
Controls,
Sensitive data.

Palabras clave:
Gestión de riesgos,
NTC-ISO/IEC 27005,
NTC-ISO 31000,
Seguridad de la información.

ABSTRACT:

Currently, organizations in all productive sectors, but mainly in government, financial services, banking, telecommunications and education, support their activities on information technologies, due to the fact that keeping business continuity is increasingly complex, as the rising threats on technologies and organizational processes, can materialize as security incidents according to the risk level and the opportune actions taken by the organization in this regard. In Colombia, risk management at corporate levels is usually achieved through standards such as NTC-ISO 27005 and NTC_ISO 31000, but worldwide the diversity of standards and criteria established for business schemes, policies, analysis and risks management, hinders the task of adopting them, due to the lack of a methodological process approach and the difficulty of having software technological alternatives to assist in this work. This article presents a review of security risk management in Colombia and the development case of a web-oriented system for risk analysis under these standards.

RESUMEN

Actualmente las organizaciones en todos los sectores productivos principalmente el gobierno/sector público, servicios financieros y banca, telecomunicaciones y educativo, soportan sus actividades en tecnologías de la información, donde mantener la continuidad del negocio cada día más complejo, dado que el aumento de amenazas sobre las tecnologías usadas y los procesos organizacionales, se pueden materializar en incidentes de seguridad de acuerdo al nivel de riesgo y las acciones oportunas que tome la organización en este sentido. La gestión de riesgos en Colombia, a nivel corporativo generalmente se asume a través de estándares como la norma NTC-ISO 27005, NTC_ISO 31000 pero a nivel global la diversidad de normas y criterios establecidos para los esquemas de negocio, las políticas, análisis y la gestión de riesgos, dificultan la tarea de asumirlo por la falta de un planteamiento de proceso metodológico y la dificultad de disponer de alternativas tecnológicas basadas en software que asistan esta labor. Este trabajo presenta una revisión de la gestión de riesgos de seguridad en Colombia y el caso de desarrollo de un sistema orientado a la web para el análisis de riesgos bajo estos estándares.

[1]MSc. in Free Software; area of network and operating system administration. Specialist in Telematic Solutions and Systems Engineer. Professor, Faculty of Basic Sciences and Engineering, Universidad de los Llanos, Villavicencio, Colombia. E-mail: felcorredor@unillanos.edu.co ORCID: https://orcid.org/0000-0002-3389-9951

[2]MSc. in Free Software, Professor, Faculty of Basic Sciences and Engineering, Universidad de los Llanos, Villavicencio, Colombia, E-mail: dfranco@unillanos.edu.co ORCID: https://orcid.org/0000-0002-6748-0729

[3]BSc. in Systems Engineering, Universidad de los Llanos, Colombia. Open Technologies Research Group – GITECX. E-mail: diego.izquierdo.dussan@unillanos.edu.co ORCID: https://orcid.org/0000-0001-6642-6096

Cite this article as: F. A. Corredor-Chavarro, D. C. Franco-Mora, D. Izquierdo-Dussan, "Implementation of cybersecurity risk analysis systems in Colombia", Visión Electrónica, vol. 2, no. 2, Special edition, 2019.. https://doi.org/10.14483/issn.2248-4728

1. Introduction

As established by the International Standards Organization (ISO) in its 27001 standard, information security focuses on "... protecting information assets and minimizing the risk from threats ...". That is why there are specific standards in the industry that define methodologies and good practices for risk management, such as ISO 27005, ISO 31000, Magerit, Octave, among others. This contrasts with the current context, where small and medium organizations do not have sufficient human, economic or technological resources to formally assume an organizational risk management methodology that allows them to mitigate risks over processes and technological threats in their Information technology infrastructure (IT).

Assuming standards is an expensive and complex process, which entails rigorous appropriation of a risk management methodology, as well as the efforts of professionals in the areas of information security and the treatment of large amounts of associated information, to analyze the security levels and take decisions to mitigate risk and improve organizational processes. However, to reduce information security risks, it is not sufficient to evaluate only from the viewpoint of processes, as the installed technological capacity entails the possibility of threats materializing directly on the computing and communications infrastructure.

There are software tools that allow to adopt some risk management methodologies, but most of them are from security consulting companies that use them in a closed and private way to offer their services. On the other hand, the few existing free software tools are outdated, do not consider the Colombian legal framework and do not have the respective software documentation. Aggravating the situation, these are only limited to the risk of processes within a specific standard and do not comprehensively and accurately assume technological threats and risks.

In this scenario, research in the field of security risk management continues and has been proposing quantitative, qualitative and hybrid approaches, as well as approaches at the level of implementation of management and analysis tools; in several of these cases, algorithms with computational intelligence. Nonetheless, no conclusive solution has been reached, as the rates of security incidents in companies continue increasing; for that reason, this project assumed the design of a solution alternative in the context of risk analysis, using multitier architecture software, based on the NTC-ISO / IEC 27005 and NTC-ISO 31000 standards, to support analysis processes of information security risks in organizations, maintaining confidentiality, availability, integrity and non-repudiation, so that Colombian companies can use it safely, to support their security risk management and lower the costs this work implies. The article is developed from the contextualization of the problem, a state of the art review, then the methodological development and the proposed architectural design and the work conclusions.

2. Problem contextualization

Currently organizations in all productive sectors, but mainly government, financial services and banking, telecommunications and education sectors, support their activities on information and communication technologies (ICT), due to the fact that the business environment of companies is increasingly complex, causing an increase in threats for technologies and organizational processes, which can materialize in security incidents, according to the risk level and the appropriate actions taken by the organizations about it. That is the reason why organizations are investing extensively in information security, especially in the item "guaranteeing the protection of business information", taking into account that digital treatment of it has greater risks of potential attacks [1].

The International Standards Organization (ISO) in its 27001 standard, defines information security as "… the protection of information against a wide variety of threats in order to ensure business continuity, minimize business risk and maximize the return on investment and business opportunities", but the context (ACIS in its Latin American Survey on Computer Security 2015) indicates that although 79% of large organizations adopt risk management standards, only 43 % of these, direct and supervise a program of information security risks regarding the standard. This survey also indicates that the most widely used standard is ISO 31000 by almost 40% of organizations.
The field of risk management assumes relevant aspects, associated with risk analysis, classification, control and mitigation; for this reason, it is essential to have technological tools that adopt the approaches of the norms and standards for risk management, but at the same time, do not require high levels of expertise to properly use the tool. This would provide a better perspective for decision making in organizations and ultimately, would help improve security in companies (by reducing risk, information security is substantially improved), reducing costs considerably [2].

In Colombia, risk management at corporate levels, is generally adopted through standards such as NTC-ISO 27005 and NTC_ISO 31000, derived from the approaches of the International Standards Organization. However, at the global level, the diversity of norms and criteria established for aspects associated with business schemes, risk policies, risk analysis and their management, make it difficult to assume one as the best, as they differ in their approaches, but above all, due to the lack of a methodological process approach to assume these activities and the difficulty of having software based technological alternatives to assist in this work. In this scenario, research in security risk management has been proposing several approaches: quantitative, qualitative and hybrid, as well as approaches related to implementation of management and analysis tools, often using fuzzy logic algorithms [3][4], computational intelligence [5], game theory [6], among others.

3. Background

Analysis and risk management through the history of mankind

Throughout history, humanity has had to deal with risks, however it was not until the 1930s that risk analysis began to be a science within the military sector. Risks have had different sources; according to the CEDIAC institute in Argentina, there are two main groups of risks: "Natural risks and risks generated by human activities".

Risks have always been present, therefore humanity has had to devise different ways to analyze and manage these risks, finding different methodologies mostly related with probability, since according to ISO 31000 (2011), risk is defined as the "effect of uncertainty on objectives". These methodologies measure risks both qualitatively and quantitatively regardless of whether or not they are counteracted [7].

When information technologies emerged, risk analysis and management took a new direction, since the use of these technologies generated new risks that were not known until now, therefore methodologies adapted to them were invented, such as Magerit, for example [8].

3.1. Legal framework

One of the most relevant references in Colombia is the CONPES 3854 document, which defines the national policy on digital security, and is focused on risk management; providing action parameters to state forces, industry, academia and society, regarding risk management in the digital environment. Likewise, the ICT ministry established the ISPM (Information Security and Privacy Model) through a library with 21 guides, to allow Colombian organizations to perform information security and risk management in a less complex way (specifically guide number 7).

Generally, legislation related to cybersecurity aspects implies some degree of legal risk that must be taken into account, as examples, Law 1273 of 2009 "about the protection of information and data", which contemplates information crimes, Law 1581 of 2012 which "establishes the general statements for the protection of personal data", Law 1704 of 2014 "transparency and the right of access to national public information", and Law 1928 of 2018 "Convention on Cybercrime that defines the application of instruments to fight effectively against these crimes, facilitating their investigation and sanction, both nationally and internationally".

3.2. Risk analysis and management through an organization's development

Taking into account that risk management is the action plan to counteract risks once they insinuate their presence and that risk analysis is the measuring (quantitative or qualitative) of these, regardless of the action plan. Organizations are placing value on identifying information security risks and action plans to counteract them, as information is the most important thing for organizations. In other words, organizations are investing heavily in information security; especially in risk analysis and management, as threats are increasing. However, the main concern of organizations is not information technologies themselves, but the employees who manipulate this technologies, as the greatest risks of information loss are generated by people [9-11].

The new generation of high-performance computers for business and research environments has proposed new challenges for risk management and analysis, since most processes have been systematized, and as management technologies are updated, so are the new tools and attack techniques [12].

Currently, in the context of risk management, there are standards such as the COSO ERM (Enterprise Risk Management) framework by the "Committee of Sponsoring Organization of the Treadway Commission", that broadens the concept of internal control; the ISO 27005 standard, oriented to risk management of information security, proposed by the International Organization for Standardization (ISO); the GRC (Governance, Risk & Compliance) model that aims to synchronize information and activities through government, risk management and GRC compliance; the ISO 31000 standard, oriented to risk management

and proposed by ISO; the Australian standard for risk management AS/NZ 4360; the methodology for risk analysis and management developed by the Higher Council for Electronic Administration known as Magerit, and the strategic planning and consulting technique for risk-based security, called Octave developed by Computer Emergency Response Team (CERT).

4.Methodological development and architecture design

The development team consists of two developers and a simple design is sought. Code should be open to modifications in any stage of development, and any developer should be able to modify it. With that in mind, Extreme Programming (XP) has been chosen as the development methodology. One important feature of XP is the adaptability of requirements at any point of the project life cycle.

Planning phase: after having analyzed the ISO 27005 and ISO 31000 standards, the tools used for the development of the information system were discussed, system characteristics and limitations, functional and non-functional requirements, as well as users involved were established. The necessary information for the methodology structure was drafted, which must integrate the aspects of ISO 27005 and ISO 31000 standards.

Design phase: System components, and possible information and user interaction flows were studied, in order to model the system under design and development standards.

Coding phase: Creation of code to comply with all the system requirements and functions defined in the two previous phases. System interfaces were created.

Test phase: the system was fully tested to verify its functioning, a test case was made based on real data from the risk management process of the Universidad de los Llanos and its results were verified.

Book writing phase: the technical and user manuals were written. This documents support the development of the project from the viewpoint of software engineering.

Planning phase: this phase consisted of
- Identification of requirements to solve the proposed problem.
- Schedule planning.
- Delegation of tasks to developers.
- Definition of functional requirements.
- Definition of non-functional requirements.
- Selection of tools to use.
- Definition of security methods to use.
- Definition of users involved in the system (roles or profiles).
- Lead auditor.
- Auditor Assistant.
- Organization representative.

4.1. Application user profiles

Each one of the user roles has a set of transactions allowed for the role. Any person or user registered in RISMATT can be a Lead Auditor, Assistant Auditor or Representative of the organization, depending on the role assigned in each audit. Users can participate in different audits with a different role in each one. The user who creates an audit automatically becomes the Lead Auditor for said audit.

Lead Auditor: A person who has created an account in RISMATT, and having created an audit, is automatically given this role. A Lead Auditor is able to:
- Add assistant auditors
- Add organization representatives
- Add risks
- Block phases of the audit
- Generate reports
- See transaction logs .
- Edit audit
- See staff members
- Edit staff members
- See risks
- Edit risks
- Delete risks
- Edit processes
- Participate in phases

Assistant Auditor: person who has a user account in RISMATT and has been assigned this role by the lead auditor of a specific audit. An assistant auditor is able to:
- Add risks
- Participate in phases

Organization representative: person designated by the organization for audit monitoring. This person is registered into the audit by the lead auditor. An organization representative is able to:
- See audit progress
- Generate reports

4.2. Technologies used

Following, the software and hardware tools used for the development of the project are presented.

4.2.1. Diagramming and Modeling
- Use cases: StarUML
- Class Diagrams: StarUML
- Sequence Diagrams: StarUML
- Relational model: ERMaster (Eclipse plugin).

4.2.2. Required Software

- *Operating system:*
- Windows 10
- *Programming language*
- PHP
- JavaScript
- AJAX
- *Libraries*
- JQuery
- chartjs
- Maatwebside laravel-excel
- *Frameworks*
- Laravel 5
- Bootstrap
- *Technologies*
- HTML5 (HyperText Markup Language, Versión 5)
- CSS3 (Cascading Style Sheets)
- *Version Control System*
- Git
- BitBucket
- SourceTree
- *Web Server*
- Apache Tomcat with XAMPP
- *Database management system*
- PostgreSQL Server 9.4
- *Database administrator*
- pgadmin3 and pgadmin4

4.3. Proposed architecture

The prototype design was created on an MVC architecture, likewise, a modular architecture was proposed, in order to achieve a better understanding of the system and facilitate its scalability. Below, the summary of modules is presented.

Module	Description
Data and file encryption	Performs symmetric cryptographic operations on the information of each organization that uses the system, likewise, it transfers files between entities. The encryption algorithm is AES.
Alerts	Sends email alerts securely.
Authentication	Two-factor authentication, with failed-attempts counter and captcha.
Access control	User profiles and associated transactions, which are verified and registered in the Database.
Inference	Statistical inference to relate the probability and impact parameters in each process.

Table 1. Summary of modules. Source: own.

The context for RSIMATT system deployment correlates the modules through the graphic representation of the architecture proposed in Figure 1.

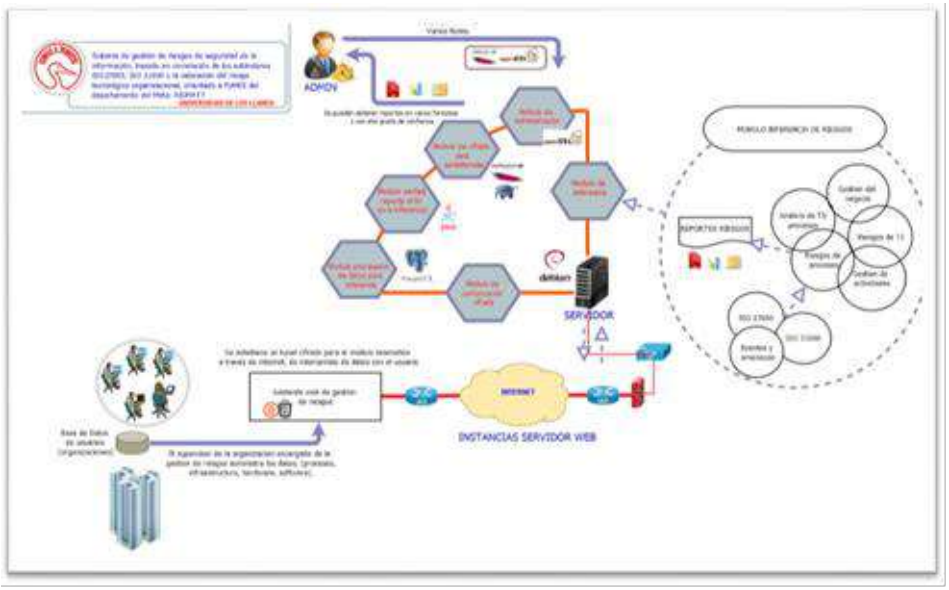

Figure 1. Proposed architecture for RISMATT. Source: own.

The development team was made up of four people: two junior analysts and two cybersecurity researchers, who established the RSIMATT architecture, data modeling and business logic, as well as the definition of the requirements and the respective use cases. (See Figure 2).

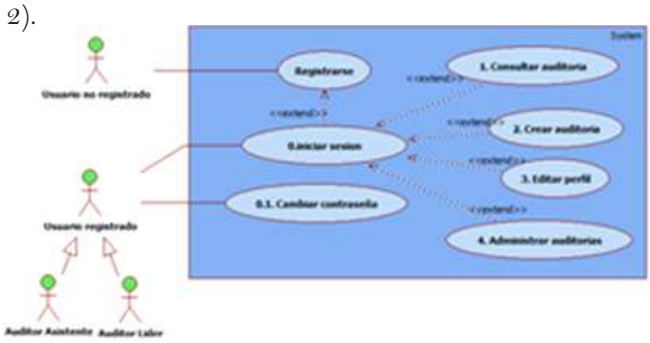

Figure 2. Rismatt General Use Case. Source: own.

5.Implementation

A multitier architecture system was implemented, using only open source technologies and following a four phase methodology for risk analysis: Phase 1. Frame of reference, Phase 2. Integration and communication, Phase 3. Context establishment and criteria definition, Phase 4. Assessment, Phase 5. Report Generation [13].

Figure 3. RISMATT startup interface. Source: own.

The information of analysis and assessment risks of an organization, is classified as highly sensitive information and must be protected under the principles of confidentiality and access control. For this reason, access is restricted by a secure login module, use case diagram is presented below.

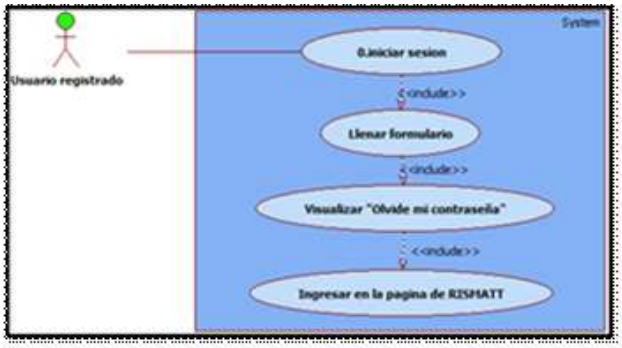

Figure 4. Use case login. Source: own.

Rismatt's secure web login interface involves password encryption with 256-bit AES in CBC mode of operation.

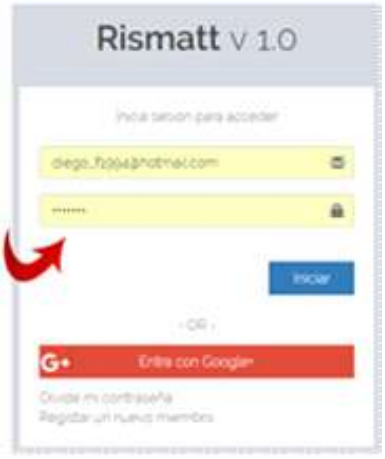

Figure 5. RISMATT Login Interface. Source: own.

Risk analysis is performed through an audit process, which guides the methodological process from audit creation to risk assessment and the respective reports.

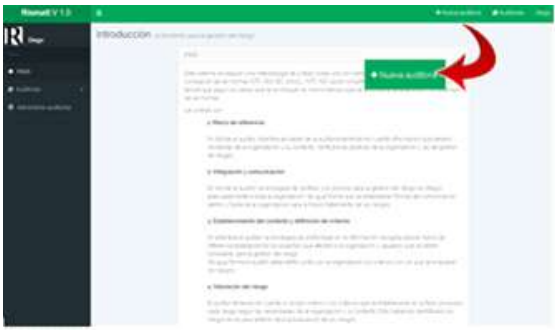

Figure 6. Start process - Risk audit. Source: own.

RISMATT audit administration capabilities were established for the Lead Auditor, from the software design process, based on the dynamics of the common development of an audit:

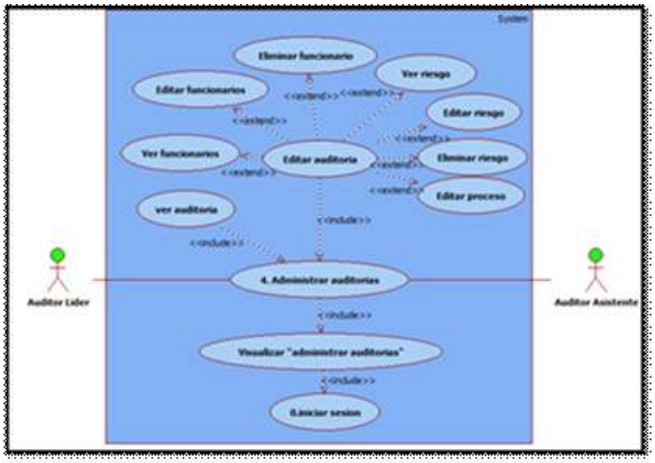

Figure 7. Use case Manage audit. Source: own.

From the viewpoint of organizational processes, it is possible to identify the risks and associate them with the respective processes, in order to subsequently classify and assess them.

Figure 8. Assignment of Risks to Processes. Source: own.

The principle of risk assessment is based on the probability / impact relationship, as stated on the standard, also associating other parameters that provide a more accurate characterization of the risk to be evaluated. Below, the interface made for this purpose is presented.

Figure 9. Risk Assessment. Source: own.

A risk classification matrix allows each evaluated risk to be located in a cell, so that through a quick overview, the auditor can begin to perceive the general state of the organization regarding information security risks.

Figure 10. RISMATT risk matrix. Source: own.

After the general audit overview presented by RISMATT, the auditor can access a more specific and detailed report about the status of each assessed risk. This reporting system is supported by graphs and statistics, which allow the organization to define controls to mitigate the impact of possible security incidents.

Figure 11. Graphic report - Risk acceptance level. Source: own.

6. Conclusions

Risk management in Colombia at corporate levels is generally assumed through standards such as NTC-ISO 27005 and NTC_ISO 31000, derived from the approaches of the International Standards Organization. At global level, on the other hand, the diversity of norms and criteria established for matters associated with business schemes, risk policies, risk analysis and their management, makes it difficult to assume one as the best, since these standards differ in their approaches, but above all, due to the lack of a methodological process approach to assume these activities and the difficulty of having software based technological alternatives to assist this work.

The software technologies available in the context focus their business model on maintaining dependence on a third party that provides consulting and advisory services in the adoption of the methodological process for risk analysis and management, meaning that while largest companies do not present difficulties to assume these costs, on the other hand, smallest and medium companies in Colombia refrain from starting these processes.

Acknowledgments

The authors express their gratitude to God and their families, who have always supported this process. Likewise, to the Universidad of the Llanos for believing in this research project called "Information security risk management system, based on correlation of standards ISO27005, ISO 31000 and the assessment of organizational technological risk. RISMATT (C01-F02-031-2016)".And other sectors to implement the cybersecurity in Colombia [13-18].

References

[1] ACIS - Asociación Colombiana de Ingenieros de Sistemas, "XIX Encuesta Nacional de Seguridad Informática," *Sistemas*, vol. 151, pp. 12-41, 2019. https://doi.org/10.29236/sistemas.n151a3

[2] M. Fugini, M. Teimourikia, and G. Hadjichristofi, "A web-based cooperative tool for risk management with adaptive security," *Futur. Gener. Comput. Syst.*, vol. 54, pp. 409-422, 2016. https://doi.org/10.1016/j.future.2015.04.015

[3] H. F. Atlam and G. B. Wills, "An efficient security risk estimation technique for Risk-based access control model for IoT," *Internet of Things*, vol. 6, 2019. https://doi.org/10.1016/j.iot.2019.100052

[4] M. M. Silva, A. P. H. De Gusmão, T. Poleto, L. C. E. Silva, and A. P. C. S. Costa, "A multidimensional approach to information security risk management using FMEA and fuzzy theory," *Int. J. Inf. Manage.*, vol. 34, no. 6, pp. 733-740, 2014. https://doi.org/10.1016/j.ijinfomgt.2014.07.005

[5] R. O. Andrade and S. G. Yoo, "Cognitive security: A comprehensive study of cognitive science in cybersecurity," *J. Inf. Secur. Appl.*, vol. 48, 2019. https://doi.org/10.1016/j.jisa.2019.06.008

[6] A. Zarreh, H. Da Wan, Y. Lee, C. Saygin, and R. Al Janahi, "Risk assessment for cyber security of manufacturing systems: A game theory approach," Procedia *Manufacturing*, vol. 38, pp. 605-612, 2019. https://doi.org/10.1016/j.promfg.2020.01.077

[7] S. K. Katsikas, Computer and Information Security Handbook. Elsevier, segunda edicion, pp 3-23, 2009.

[8] E. Vicente, A. Mateos, and A. Jiménez-Martín, "Risk analysis in information systems: A fuzzification of the MAGERIT methodology," *Knowledge-Based Syst.*, vol. 66, pp. 1-12, 2014. https://doi.org/10.1016/j.knosys.2014.02.018

[9] C. A. Ortega Ruiz, "Inclusión de las TIC en la empresa colombiana," *Suma Negocios*, vol. 5, no. 10, pp. 29-33, 2014. https://doi.org/10.1016/S2215-910X(14)70006-0

[10] E. J. Gálvez Albarracín, S. C. Riascos Erazo, and F. Contreras Palacios, "Influencia de las tecnologías de la información y comunicación en el rendimiento de las micro, pequeñas y medianas empresas colombianas," *Estud. Gerenciales*, vol. 30, no. 133, pp. 355-364, 2014. https://doi.org/10.1016/j.estger.2014.06.006

[11] M. L. Guerrero Julio and L. C. Gómez Flórez, "Gestión de riesgos y controles en sistemas de información: del aprendizaje a la transformación organizacional," Estud. Gerenciales, vol. 28, no. 125, pp. 87-95, 2012. https://doi.org/10.1016/S0123-5923(12)70011-6

[12] A. A. Castro and S. C. Riascos Erazo, "Direccionamiento estratégico apoyado en las tics," Estud. Gerenciales, vol. 25, no. 111, pp. 127-143, Apr. 2009. https://doi.org/10.1016/S0123-5923(09)70074-9

[13] O. Ospina Zuñiga, G. García Cobas, J. Gordillo Rivera and K. Tovar Hernández, "Assessment of Murky Water and its Conductivity During Dry and Rainy Seasons in Combeima River (Ibagué, Colombia)", Ingeniería Solidaria, vol. 12, no. 19, pp. 19-36, 2016. . https://doi.org/10.16925/in.v12i19.1191

[14] J. A. Vargas, J. Arango and L. G. Isaza Domínguez, "Instructional Strategy to Train Professors from the Civil Engineering Program in the Use of Information and Communications Technologies (ICTS) at the Villavicencio Campus of the Universidad Cooperativa de Colombia", Ingeniería Solidaria, vol. 10, no. 17, pp. 161-174, 2014. https://doi.org/10.16925/in.v9i17.829

[15] A. P. Becerra Quiroz, A. L. Buitrago Coca and P. Pinto Baquero, "Sustainability of sugar cane bagasse utilization in Valle del Cauca, Colombia", Ingeniería Solidaria, vol. 12, no. 20, pp. 133-149, 2016. https://doi.org/10.16925/in.v12i20.1548

[16] E. de Avila y A. Díaz, "Articulación del sistema ferroviario con los puertos marítimos y fluviales colombianos como alternativa estratégica para mejorar la competitividad internacional". Conocimiento Global, vol. 2, no. 1. pp. 69-73. 2017. https://conocimientoglobal.org/revista/index.php/cglobal/article/view/18

[17] J. Machado, "Administración de residuos una política de gestión ambiental en la generación de valor empresarial". Enfoque Disciplinario, vol. 3, no. 1, pp. 72-85. 2018. https://enfoquedisciplinario.org/revista/index.php/enfoque/article/view/13

[18] J. Machado,"Administración de residuos una política de gestión ambiental en la generación de valor empresarial". Enfoque Disciplinario, vol. 3, no. 1, pp. 72-85. 2018. http://enfoquedisciplinario.org/revista/index.php/enfoque/article/view/13