Revista Ingenio
UFPS Ocaña
"Journal of Engineering Sciences"

Original Article Doi: https://doi.org/10.22463/2011642X.3808

Information security model in line with the principles of IT Governance for the industrial manufacturing sector

Modelo de seguridad de la información bajo los principios de Gobierno TI para el sector industrial manufacturero.

MSc. (c) Jenis del Carmen Sagbini Echávez[1], Ph.D. Torcoroma Velásquez Perez[2], Ph.D. (c) Edwin Espinel Blanco[3]

1 Universidad Francisco de Paula Santander Ocaña, Estudiante de Maestría Gobierno TI, Vía Acolsure Sede el Algodonal, Ocaña-Norte de Santander, Colombia, Orcid: https://orcid.org/0009-0005-9484-358X, Email: jdsagbinie@ufpso.edu.co
2Universidad Francisco de Paula Santander Ocaña, Grupo de Investigación GITYD, Vía Acolsure Sede el Algodonal, Ocaña – Norte de Santander, Colombia, Orcid: https://orcid.org/0000-0002-2968-2338, Email: tvelaszquep@ufpso.edu.co
3Universidad Francisco de Paula Santander Ocaña, Director del Plan de Estudios de Ingeniería Mecánica - Vía Acolsure Sede el Algodonal, Ocaña – Norte de Santander, Colombia, Orcid: https://orcid.org/0000-0003-4479-2874, Email: planim@ufpso.edu.co

Cite this article as: J.C. Sagbini-Echávez, T. Velásquez-Pérez y E. Espinel-Blanco, "Information security model in line with the principles of IT Governance for the industrial manufacturing sector" Rev. Ingenio, vol. 21, n°1, pp. 9-12, 2024, doi: https://doi.org/10.22463/2011642X.3808

Received date: 15 de marzo, 2023
Approval date: 29 de agosto de 2023

Keywords:

Information, Industry, IT Governance, Security, Technology

ABSTRACT

In this article, an information security model is proposed under the principles of IT Governance for the industrial manufacturing sector. The investigation began with an analysis of the standards required to be able to align Information Technology to the strategic direction of the company; verifying in this way, the most applicable schemes for the structuring of the model. Subsequently, a quantitative methodology with a descriptive scope was used, which allowed the definition of the model with the aim of guaranteeing the confidentiality, integrity and availability of the information. The model was satisfactorily validated by subject experts, guaranteeing its applicability.

Palabras clave:

Información, Industria, Gobierno TI, Seguridad, Tecnología

RESUMEN

En el presente artículo se propone un modelo de seguridad de la información bajo los principios de Gobierto TI para el sector industrial manufacturero. La investigación inició con un análisis de los estándares requeridos para poder alinear la tecnología de la información al direccionamiento estratégico de la empresa; verificando de esta manera, los esquemas más aplicables para la estructuración del modelo. Posteriormente, se utilizó una metodología de tipo cuantitativo con un alcance descriptivo, que permitió definir el modelo con el objetivo de garantizar la confidencialidad, integridad y disponibilidad de la información. El modelo fue validado satisfactoriamente por expertos del tema garantizando su aplicabilidad.

1. Introduction

The overriding goal of companies is to ensure their sustainability, which involves prioritizing consumer security, promptly addressing their needs, and effectively managing production costs [1]. The utilization of ICTs in organizations, particularly in manufacturing industries, has resulted in the reformation of processes, including enhanced resource planning, decreased costs, improved mobility, and accelerated service provision, facilitating integration into a dynamic and evolving economy. This has thus enabled an increased dependence on ICT (Information and Communication Technologies) in all aspects of its operations.

The interactions between production and business processes take place through the integration of formal knowledge, as well as the digitization of procedures, information, and resource behavior models enabling automatic or semi-automatic decision-making [2].

IT governance is a component of corporate governance. This refers to the framework of relationships and procedures that guide and oversee a company's operations, with the aim of achieving its objectives and creating value, while effectively managing the balance between risk and return on investments in information technology and its associated processes [3]. It is hence necessary for an organization aiming to effectively oversee its technological assets to consider implementing a well-designed plan and structure of a model that can efficiently manage them. This will enable the organization to make informed decisions aligned with its

Corresponding Author
Email: jdsagbinie@ufpso.edu.co (Jenis del Carmen Sagbini Echávez)

strategic corporate governance.

The content of the essential elements of the Information Security Model for industrial manufacturing companies was established, in which methodologies and standards such as the Balance Score Card, COBIT 5.0, and ISO 27002:2013, and with an overarching objective to effectively control all organizational processes and ensure the confidentiality, integrity, and availability of information. This is because the assurance of the integrity and security of stored data is not always guaranteed. [4]

2. Methodology

In this research, specific numerical data was gathered, which was organized in a notable statistical manner. Also, the breadth of the analysis was descriptive as it focused on examining the actuality of circumstances, events, individuals, organizations, or communities that had been studied. In addition, the research extended beyond mere description, as it aimed to provide the most significant trait of a particular event or circumstance and its analysis had to be defined together with the associated processes. [5] [6]

The population and sample are defined as companies in the industrial manufacturing sector, specifically SMEs based in Barranquilla, engaged in producing electrical and electronic items, categorized according to the DIAN with code 270, which represents the manufacture of electrical appliances and equipment. Within this category, the subcategory 2790 is selected. Information was gathered using digital instruments, including surveys and interviews, with a significant representation narrowed down to participants who were leaders in the IT sector [7] of SMEs in the industrial manufacturing sector in the city of Barranquilla.

To conduct the analysis in this research, a thorough documentary research was required, which involved searching for a specific response by examining relevant papers [8]. Each of the stated objectives was compared with different criteria and created a comparative table, which enabled us to deliver a response based on the data gathered. Similarly, the essential components of standards related to information security that were relevant to the manufacturing industry were based on the tabulated available data, as well as its systematic organization.

3. Discussion and Results

The research outcomes began by creating a comprehensive comparative table that enabled us to draw conclusion from the standards on information security procedures, including the ISO bundle of standards (27000, 27001, 27002, 27005) [9], ITIL V3 2011, and COBIT 5.

After analyzing the comparative table and considering the purpose of the study, it was determined that two standards, ISO 20001 and the comprehensive work scenario referred to as COBIT 5, would be utilized as references for IT governance and management.

Based on the specific standards and the results of applied questionnaires to the leaders of the Information Technology department in each selected manufacturing company, the shake-up of every element comprising the information security model for industrial manufacturing organizations was initiated.

During this stage, the main component identified was the interested parties or stakeholders, which can be either corporations or individuals and who have an impact on or may be impacted by the company's operations. The company must consider all stakeholders, as customers will only purchase products that meet their desires, needs, and requirements in terms of price, quality, service, and quickness. That is, shareholders will not invest in a company that fails to meet their demands for dividends or capital gains. Also, society will not tolerate companies that do not fulfill their legal obligations and meet expectations for quality of life. Professionals will not engage in activities or contribute their knowledge nor will they strive to design and manage the different organizational processes unless the company satisfies their desires and demands for job satisfaction. Ultimately, suppliers will not continue to provide their knowledge, skills, and resources to a company that does not offer them the opportunity to obtain a reasonable profit. [10]

Subsequently, the operational procedures of these companies were recognized, which encompass the essential activities of the organization as a manufacturer of products, serving as the core element of its value chain.

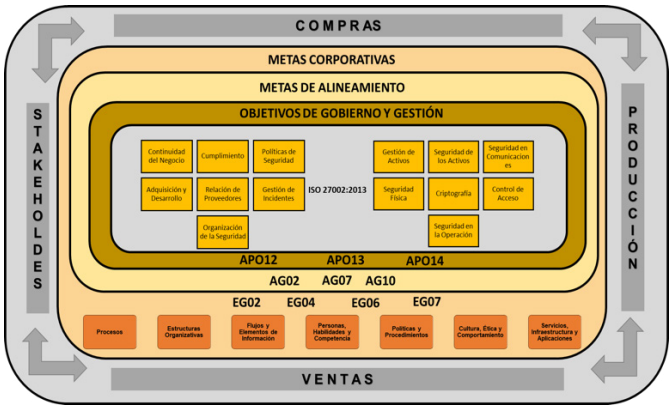

Figure 1. Information Security Model based on the IT principles for the manufacturing industry.

The operations were centered around the procedures APO12 - Risk Management, APO13 - Security Management, and APO14 - Data Management. This was established because these processes are intrinsically connected to information security, which mainly focuses on information management and the governance of all IT assets. As a result, an Information Security Management System was developed to define, operate, and monitor these processes.

Manufacturing companies employ clearly defined plans to implement a systematic and long-term approach to their production systems. These mission processes were also considered within the context of this model, which is connected to the creation of value for the client, specifically, Purchasing, Production, and Sales that will deliver the desired outcome for the organization, as they serve its purpose.

Using all the gathered data, a comprehensive information security model was developed specifically for industrial manufacturing companies:

The structure used to set corporate goals gives relevant information regarding each of the governance components that contribute to the effective functioning of the company's governance system. These components can interact and come in different sorts, as illustrated in Figure 1.

The process component is dominant as it covers a series of approaches and actions aimed at achieving specific goals and producing outputs that contribute to the fulfillment of all IT-related objectives.

The Organizational Structures component plays a crucial role in the decision-making process within an organization, whereas The Principles, Policies, and Frames of Reference component operationalizes the desired behavior for day-to-day management.

The information component pertains to the central core or foundation of any organization; it is therefore the entity that is generated and utilized. COBIT is founded on the essential information required for the effective and valuable operation of the company's governance system. On the other hand, an often overlooked yet crucial element in the effectiveness of governance and management activities is the influence of Culture, Ethics, and Behavior, which has to do with the actions of individuals inside an organization. [11]

The People, Skills and Competencies component is essential for making informed decisions, as well as implementing necessary corrections, and completing all tasks. Lastly, Infrastructure and Applications Services span the same components to establish a governance system for the company's I & T processing.

In regards to the Alignment Goals, "COBIT 5 alignment is considered to be the result of all governance and management activities" [12] and [13]. This is the reason why it was included in this model. The specific Alignment Goals are as follows: AG02 focuses on risk management linked to I&T, AG07 addresses information security, processing infrastructure, applications, and privacy, and AG10 emphasizes the quality of information connected to I&T management.

The governance and management objectives APO12 Manage risk, APO13 Manage security, and APO14 Manage data are located within the model.

The IT Governance Model's business goals encompass EG02 - Risk Management, EG04 - Quality of Financial Information, EG06 - Business Service Continuity and Availability, and EG07 - Quality of Management Information.

EG02, refers to risk management, whose metrics include:

a. Proportion of essential company goals and services included in the risk assessment
b. The ratio of relevant mishaps that were not identified in the risk assessment to the total number of incidents.
c. Frequency of risk profile updates.

Activities to be performed can also be monitored with the ability to recognize, assess, and consistently mitigate the risks associated with I&T. To protect information security through risk management constitutes the overarching goal of a company dealing with its information.

The EG04 Quality of Financial Information component corresponds to one of the business goals included in the model's metrics.

a. Surveys measuring the satisfaction of individuals impacted by the company's financial information, specifically evaluating the level of transparency, comprehension, and correctness.
b. The precise financial consequences of failing to comply with all financial requirements.

The quality of financial information is a key objective for management, specifically under objective AP014, which falls under the broader category of data management and allows investors and/or managers of a manufacturing company to make decisions based on reliable information meeting some criteria, which should be well-structured, clear, and easily understandable.

Business Service Continuity and Availability in AP013 include the next business metrics:

a. Total count of customer service interruptions or

otherwise business processes resulting in substantial mishaps.
b. Financial impact of accidents on the business
c. The amount of time for company operations that cannot be carried out due to unexpected service disruptions
d. The proportion of complaints is based on the established service availability targets.

The EG07 component, which is related to the quality of management information, is in line with AP014, which pertains to the management of data. There are some model metrics to manage business goals effectively.

a. The level of satisfaction of the board of directors and executive management over the adequacy of information for decision-making.
b. Number of occurrences resulting from flawed corporate decisions made, based on incorrect data.
c. The length required to deliver the information that facilitates efficient decision-making in business.
d. Timeliness of management information

4. Conclusions

The study identified the most commonly cited information security practices, which include COBIT 5.0 and the ISO 27000:2017, ISO 27001:2015, ISO 27002:2017, and ISO 27005:2011 standards. Also, it focused on determining the fundamental components that are relevant to the manufacturing industry. Similarly, an examination was conducted on the various procedures implemented within manufacturing industrial companies.

Based on the frame of reference COBIT 5.0:2019 and ISO 27000 bundle of standards, it was feasible to organize the essential elements in IT Governance to create an information security model, specifically tailored for organizations operating in the industrial manufacturing sector. This structure originated from the Stakeholders, encompassing the mission processes, business goals, alignment goals, and governance and management objectives of the company.

The suggested model was validated using the Delphi Model as a reference. This process involved a panel of 9 experts with Information and Communication Technology backgrounds and a considerable understanding of methodology and experimentation. This confirms that the suggested model meets all the fundamental criteria, so it is advisable to implement it in organizations operating in the industrial manufacturing sector.

5. Acknowledgments

We express our gratitude to all those who provided their expertise and experience for the advancement of this research, as well as to the members of our family who wholeheartedly supported the completion of this chapter of our professional training.

6. References

[1] E. A. Chacón-Ramírez, J. J. Cardillo-Albarrán, y J. Uribe-Hernández, "Industria 4.0 en América Latina: Una ruta para su implantación," Revista Ingenio, vol. 17, n° 17, pp. 28-35, 2020, doi: https://doi.org/10.22463/2011642X.2386

[2] J. Uribe-Hernández, L. Ávila-Roa, y E. A. Chacón-Ramírez, "Sistema de gestión de energía bajo el paradigma de Industria 4.0," Revista Ingenio, vol. 1, n° pp. 33-40, 2021, doi: https://doi.org/10.22463/2011642X.2780

[3] I. L. MuñozPeriñán, Gobierno de TI Estado del arte, Cali: EditorSyT@icesi.edu.co, 2011.

[4] G. A. Verjel-Clavijo y A. M. Guerrero-Bayona, "Ciudad inteligente: mejoramiento de la seguridad ciudadana a través del uso de nuevas tecnologías," Revista Ingenio, vol. 20, n°1, pp. 32-39, 2023, doi: https://doi.org/10.22463/2011642X.3510

[5] F. Universia, "Tipos de Investivación Descriptiva-Exploratoria Explicativa", universia.cr, Buenos Aires, Argentina, 2017.

[6] S. Monkey, "Diferencia en Investigación Cuantitativa y Cualitativa", Survey, Monkey, Barcelona, España, 2023.

[7] N. Aguilar, "Modelo de Seguridad de la Información para Instituciones de Educación Superior. Ocaña, Norte de Santander", Ocaña, Norte de Santander, 2019.

[8] S. E. Ackerman, "Metodología de la investigación", Buenos Aires, Argentina: Ediciones del Aula Taller, 2013.

[9] I.C.d.N.T.y.Certificación,NORMATÉCNICANTC-ISO/IEC., 2016.

[10] P. Lorca Fernández, "La creación de valor en la empresa y los "stakeholders"", Barcelona, 2004.

[11] ISACA, "Marco de Referencia COBIT:2019 Objetivos de Gobierno TI.", 2019.

[12] ISACA, "COBIT 5, Un Marco de Negocio para le Gobierno y la Gestión de las TI de la Empresa", 2012.

[13] L. H. M.-R. R. Pablos Heredero, Organización y Transformación de los Sistemas de Información en la Empresa, Madrid: ESIC, 2019, p. 401.