Revista Ingenio
UFPS Ocaña
"Journal of Engineering Sciences"

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

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

Information security model under IT Governance principles for the manufacturing industry sector

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*
[2]*Universidad 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*
[3]*Universidad 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*

Cómo citar: J.C. Sagbini-Echávez, T. Velásquez-Pérez y E. Espinel-Blanco, "Modelo de seguridad de la información bajo los principios de Gobierno TI para el sector industrial manufacturero" *Rev. Ingenio*, vol. 21, n°1, pp. 9-12, 2024, doi: https://doi.org/10.22463/2011642X.3808

Fecha de recibido: 15 de marzo, 2023
Fecha aprobación: 29 de agosto de 2023

RESUMEN

Palabras clave:

Información, Industria, Gobierno TI, Seguridad, Tecnología

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.

ABSTRACT

Keywords:

Information, Industry, IT Governance, Security, Technology

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.

1. Introducción

Las empresas tienen como principal objetivo su sostenibilidad, asociado con la seguridad de sus clientes, respondiendo a sus necesidades de manera rápida y manteniendo los costes de producción acotados. [1] Esto ha hecho que el uso de las TIC en las empresas, más concretamente, industriales manufactureras, ha generado transformación de los procesos: mejor planificación de los recursos, disminución de costos, aumento de movilidad y hay rapidez en la prestación de servicios logrando una facilidad en la inserción de una economía dinámica y cambiante. Todo ello ha permitido una mayor dependencia de las TIC (Tecnologías de la Información y las Comunicaciones) en el interior de todos sus procesos.

Las interacciones entre procesos de producción y procesos del negocio se dan por la incorporación del conocimiento formal mediante la digitalización de procedimientos, información y modelos de comportamiento de recursos, lo que permite permite la toma de decisiones de manera automática o semiautomática. [2]

El gobierno de TI hace parte del gobierno empresarial. Se define como una estructura de relaciones y procesos para dirigir y controlar la empresa hacia el logro de sus objetivos, por medio de agregar valor, al tiempo que se obtiene un balance entre el riesgo y el retorno sobre las TI y sus procesos. [3] Es por ello, que es necesario para una organización que desee gestionar sus recursos tecnológicos pensar en tener un adecuado plan de diseño y estructura de un modelo capaz de gestionarlos para que de esta forma, se logren tomar las decisiones acertadas basadas en una alineación estratégica del gobierno corporativo.

Autor para correspondencia
Correo electrónico: jdsagbinie@ufpso.edu.co (Jenis del Carmen Sagbini Echávez)

En el presente proyecto, se estableció el contenido de los elementos esenciales del Modelo de seguridad de la información para empresas industriales manufactureras tomando como referentes metodologías y estándares, entre ellos: el Balance Score Card, COBIT 5.0 y la ISO 27002:20013, con el gran objetivo de lograr controlar efectivamente todos los procesos organizacionales y garantizando una confidencialidad, integridad y disponibilidad de la información. Lo anterior, se debe a que la integridad y la seguridad de los datos almacenados no siempre está garantizada. [4]

2. Metodología

En esta investigación, se recopiló información concreta de tipo cuantitativa, la cual fue estructurada de manera estadística notable. Su alcance fue tipo descriptivo debido a que se analizó la realidad de situaciones, eventos, personas, grupos o comunidades que se abordaron. En este tipo de investigación la cuestión fue mucho más allá del nivel descriptivo; ya que consistió en plantear lo más relevante de un hecho o situación concreta y se debió definir su análisis y los procesos que involucraron el mismo. [5] [6]

En la definición de la población y muestra, se identificaron las empresas las empresas del sector industrial manufacturero tipo MiPyme ubicadas en la ciudad de Barranquilla que se dedican a la producción de artículos eléctricos y electrónicos, categorizados según la DIAN con el código 270 – Fabricación de aparatos y equipo eléctrico que tienen varias subcategorías donde se selecciona la subcategoría 2790 –. Se utilizaron instrumentos digitales de recolección de información como encuestas y entrevistas tomando una representación significativa que consistió en todos aquellos líderes del área de TI [7] de las empresas categorizadas como MiPymes cuyas actividades pertenecen al sector industrial manufactureras de la ciudad de Barranquilla.

Para la realización del análisis en esta investigación, fue necesaria una investigación documental exhaustiva, considerada una búsqueda de una respuesta específica a partir de la indagación en documentos. [8] Se tomaron a cada uno de los objetivos establecidos relacionándolos en un cuadro comparativo de los diferentes estándares y esto permitió dar respuesta a partir de los datos encontrados. Igualmente, se seleccionaron los elementos requeridos de estándares asociados con seguridad de la información aplicables al sector manufacturero basados en la tabulación de los datos hallados, así como también a la exploración de los datos ordenadamente.

3. Resultados y discusión

Los resultados de la investigación se iniciaron con la elaboración de un cuadro comparativo representativo que permitió sacar las conclusion del estudio de todos aquellos estándares que hacen relación a las prácticas de seguridad de la información: familia de normas ISO (27000, 27001, 27002, 27005) [9], ITIL V3 2011 y el COBIT 5.

Después de estudiar el cuadro comparativo y teniendo en claro el objetivo estudiado, se llegó a la conclusión que se trabajarían como referentes dos estándares: la norma ISO 20001 y escenario de trabajo integral denominado COBIT 5 para la gobernaza y gestión de TI.

Estos estándares seleccionados y con los resultados de las encuestas aplicadas a cada uno de los líderes del área de Tecnologías de Información de cada empresa manufacturera seleccionada, se inició la estructuración de todos los elementos que conformarían el modelo de seguridad de la información para las empresas industriales manufactureras.

En esta fase, se reconocieron como principal elemento, las partes interesadas o stakeholders que pueden ser empresas o personas y que afectan o pueden ser afectados a partir de las actividades que desarrolla la empresa. Todos los stakeholders deben ser considerados por la empresa, porque los clientes no comprarán productos que no respondan a sus deseos, necesidades o exigencias de precio, calidad, servicio y rapidez; los accionistas no seguirán invirtiendo en la empresa que no satisfaga sus demandas con respecto a los dividendos o ganancias de capital; la sociedad no tolerará empresas que no cumplan sus obligaciones legales y sus expectativas referentes a la calidad de vida; los profesionales no desarrollarán sus actividades y conocimientos, ni harán el esfuerzo requerido para diseñar y gestionar los diferentes procesos de la organización, a menos que ésta dé respuesta a sus deseos y exigencias relativas a la satisfacción en el trabajo; por último, los proveedores no continuarán suministrando sus conocimientos, habilidades y recursos a la empresa que no les facilite la oportunidad de obtener un beneficio razonable. [10]

A partir de allí, se identificaron los procesos misionales de este tipo de empresas, que corresponde a las funciones sustantivas de la entidad como productora de bienes como eje central de su cadena de valor.

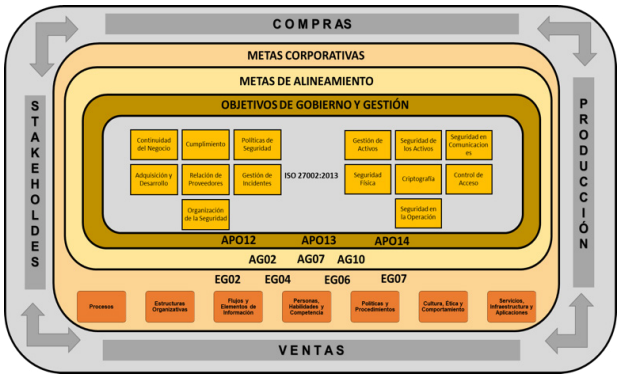

Figura 1. Modelo de Seguridad de la Información bajo los principios de TI para el sector industrial manufacturero.

Las actividades fueron enfocadas en los procesos APO12- Gestionar el riesgo, APO13-Gestionar la seguridad y APO14-Gestionar los Datos. Se estableció ello, debido a que estos procesos están vinculados directamente con la seguridad de la información cuya finalidad fundamental está orientada hacia el manejo de la información y a la regulación de todos los activos informáticos, razón por la cual, se logró edificar la definición, la operación y el monitoreo de un Sistema de Gestión de la Seguridad de la Información.

Las empresas manufactureras tienen estrategias bien definidas que permiten un planteamiento estructurado a largo plazo de un sistema de producción. Estos procesos llamados misionales, también se contemplaron en el marco de este modelo. Ellos están relacionados con la generación de valor direccionado para el cliente, en este caso, son Compras, Producción y Ventas quienes proporcionarán el resultado previsto por la empresa debido a que cumplirá su razón de ser.

A partir de toda la información obtenida, se configuró el diseño del siguiente modelo de seguridad de la información para empresas industriales manufactureras:

La estructura usada para detallar las metas corporativas entrega información reelevante con cada uno de los componentes de gobierno que son factores que apoyan al buen funcionamiento del sistema de gobierno de la empresa. Estos componentes logran interactuar y son de diversos tipos como se observa en la Figura 1.

El componente procesos es el más común porque describe una serie de métodos y acciones con orden que permiten obtener objetivos determinados y producir salidas contribuyendo a la consecución de todos los objetivos que están relacionados con las TI.

El componente Estructuras Organizativas son elementos claves para la toma de decisiones en una empresa. Quien convierte el comportamiento deseado en una aplicación práctica para la gestión diaria es el componente denominado Principios, Políticas y Marcos de Referencia.

El componente información tiene que ver con el núcleo principal o eje cental en cualquier organización, es la unidad que que es producida y utilizada. COBIT se fundamenta en la información necesaria para el funcionamiento competente y valioso del sistema de gobierno de la empresa. El componente que es subestimado como un factor de éxito en todas las actividades de gobierno y gestión es Cultura, Ética y Comportamiento, que hace relación a los individuos que actúan en una organización. [11]

El componente Personas, Habilidades y Competencias, hacen parte de las necesidades para la toma decisiones adecuadas, ellevar a cabo medidas correctivas y completar cabalmente todas las actividades. Por último, los Servicios, Infraestructura y Aplicaciones, involucra esos mismos elementos para brindar a la empresa un sistema de gobierno para el procesamiento de I & T.

Con respecto a las Metas de Alineamiento, “In COBIT 5, alignment is considered to be the result of all governance and management activities” (en COBIT 5, se considera el alineamiento como el resultado de todas las actividades de gobernanza y gestión) [12], [13] .Por lo que esta expresión muestra claramente que el alineamiento es considerado como todo aquel resultado de todas las actividades de gobernanza y gestión; razón por la cual, se incluyó en el presente modelo. Las Metas de Alineamiento estructuradas son: AG02 Gestión de riesgo relacionado con I&T, AG07 Seguridad de la información, infraestructura de procesamiento, aplicaciones y privacidad, AG10 Calidad de la Información sobre gestión de I&T.

En el interior del modelo se encuentran se localizan los objetivos de gobierno y gestión APO12 Gestionar el riesgo, APO13 Gestionar la seguridad y APO14 Gestionar los datos.

Las metas empresariales involucradas en el Modelo de Gobierno de TI corresponden a: EG02 -Gestión del riesgo; EG04-Calidad de la información financiera; EG06 – Continuidad y disponibilidad del servicio del negocio y EG07 Calidad de la Información sobre Gestión

EG02, corresponde a la gestión del riesgo, cuyas métricas, involucran:

a. Porcentaje de objetivos y servicios críticos del negocio, cubiertos por la evaluación de riesgos
b. Proporción de percances con reelevancia que no se identificaron en la evaluación de riesgos frente al total de incidentes
c. Frecuencia de actualización del perfil del riesgo.

Igualmente se pueden observar las actividades a realizar con el nivel de capacidad para poder identificar, evaluar y reducir continuamente los riesgos que tienen relación con I&T. El mayor objetivo para una organización que trabaja con su información, es salvaguardar la seguridad de la información gestionando el riesgo.

El componente EG04 Calidad de la Información Financiera correspondiente a una de las metas empresariales cuyas métricas del modelo se contemplan:

a. Encuestas de satisfacción de las partes afectadas con respecto al nivel de transparencia, comprensión y precisión de la información financiera de la empresa.
b. Costo real del incumplimiento con respecto a todas las regulaciones financieras.

La Calidad de la información financiera, como meta empresarial alineada con el objetivo de gestión AP014 que hace parte de gestionar los datos permite que las decisiones que toman los inversores y/o gerentes de una empresa

manufacturera se basa en información confiable y que cumpla con requisitos donde esté bien estructurada, clara y de forma entendible.

EG06 Continuidad y Disponibilidad del Servicio del Negocio en AP013 contiene las siguientes métricas empresariales:

a. Número de interrupciones del servicio al cliente o en su defecto, de procesos de negocio que han causado percances significativos
b. Costo de incidentes para el negocio
c. Cantidad de tiempo de procesamiento de negocio perdido debido a interrupciones del servicio no planificadas
d. Porcentaje de quejas en función de los objetivos de disponibilidad del servicio acordados

El componente EG07 Calidad de la Información sobre Gestión. Este componente está alineado con la AP014 que corresponde a gestionar los datos. En él existen las siguientes métricas modelo para gestionar las metas empresariales:

a. Grado de complacencia del consejo de administración y la dirección ejeutiva con toda la información necesaria para la toma de decisiones
b. Cantidad de incidentes causados por resoluciones equivocadas de negocio basadas en información no precisa
c. Tiempo que se tarda en dar la información que respalde la toma de decisiones de negocio eficaces
d. Puntualidad de la información sobre gestión

4. Conclusiones

Los estándares más referenciados de prácticas de seguridad de la información se lograron identificar, tomando referentes el COBIT 5.0 y el grupo de normas ISO 27000:2017, ISO 27001:2015, ISO 27002:2017, ISO 27005:2011; analizando los componentes esenciales que son aplicables al sector de la industria manufacturera. Igualmente se estudiaron los diferentes procesos establecidos en el interior del tipo de organizaciones industriales manufactureras.

Con base al marco de referencia COBIT 5.0:2019 y a la familia de normas ISO 27000, se logró estructurar los componentes necesarios en Gobierno TI para el diseño del modelo de seguridad de la información para empresas en el sector industrial manufacturero. Esta estructura se inició con los *Stakeholders,* los procesos misionales de las empresas, metas empresariales, metas de alineamiento y los objetivos de gobierno y gestión.

Tomando como referencia el Modelo Delphi, se logró hacer la validación del modelo propuesto contando con la participación de un panel de 9 expertos con perfiles en Tecnologías de la Información y Comunicación y con amplios conocimientos metodológicos y experimentales. Esto pudo establecer que el modelo propuesto cumple con todas las características básicas, por lo tanto, es recomendable para ser aplicado a empesas que pertenecen al sector industrial manufacturero.

5. Agradecimientos

Se agradece a todas las personas que apoyaron aportando sus conocimientos y experiencia para el desarrollo de esta investigación, así como las personas del círculo familiar quienes apoyaron incondicionalmente la culminación de esta fase de preparación profesional.

6. Referencias

[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, NORMA TÉCNICA NTC-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.