ISSN impreso 1996-6660 / ISSN online 2519-5719
DOI: https://doi.org/10.31381/perfiles_ingenieria.v18i18.5399

Efectos de la implementación de un SGSI basado en la norma ISO 27001 para las organizaciones

Effects of the implementation of an ISMS based on the ISO 27001 standard for organizations

Jamil Alberto Panaqué Dominguez[1]
Yerson Gabriel Lizárraga Caipo[2]
Alberto Mendoza de los Santos[3]

RECIBIDO: 10 de mayo del 2022
ACEPTADO: 12 de agosto del 2022

RESUMEN

La protección de los datos es una figura sobresaliente en la realidad, en el dominio de las redes y comunicaciones, por lo que es significativo detallar con resultados integrales que permitan ejecutar de manera eficiente las advertencias informáticas que tratan de complicar los recursos en los servicios o aprovecharse con información privada.

La vigente investigación tiene como finalidad desarrollar una exploración sistemática basada en los efectos de la aplicación de la norma ISO 27001 en las diferentes organizaciones, públicas y privadas, empresas y microempresas, pymes y mypes, las cuales están comprendidas entre el 2016 y el 2021.

Los repositorios de acceso abierto empleadas fueron Alicia, Dialnet Plus, Redalyc y Scielo.

Asimismo, los escritos se ordenaron por tiempo de difusión, lengua, lugar de la publicación y se concluyó que la aplicación de un procedimiento de seguridad de los datos contribuye verdaderamente en los siguientes aspectos: disponibilidad, confidencialidad e integridad; determinar los riesgos, vulnerabilidades y amenazas en los procesos; comprensión de las destrezas en la seguridad de los datos, e incremento de la confianza y progreso de la imagen corporativa.

Palabras clave: ISO 27001, seguridad de la información, empresas, tecnología, SGSI

ABSTRACT

Data protection is an outstanding figure in reality, in the domain of networks and communications, which is why it is significant to detail with comprehensive results that allow the efficient execution of computer warnings that try to complicate the resources in the services or take advantage of private information.

The current research aims to develop a systematic exploration based on effects of the application of the ISO 27001 standard in different organizations, public and private, companies and micro-enterprises, SMEs and mypes, which are between 2016 and 2021. The open access repositories used were ALICIA, DIALNETPLUS, REDALYC, SCIELO. Likewise, the writings were ordered by time of diffusion, language, place of publication and it was concluded that the application of a data security procedure truly contributes to the following aspects: availability, confidentiality and integrity; Determine the risks, vulnerabilities and threats in the processes; understanding of the skills in data security increasing the confidence and progress of the corporate image.

Keywords: ISO 27001, information security, companies, technology, ISMS, implementation

[1]Universidad Nacional de Trujillo, Estudiante de Ingeniería de Sistemas, <jpanaque@unitru.edu.pe>, ORCID: 0000-0003-4453-3610
[2]Universidad Nacional de Trujillo, Estudiante de Ingeniería de Sistemas, <ylizarraga@unitru.edu.pe>, ORCID: 0000-0003-3104-6864
[3]Universidad Nacional de Trujillo, Senior Lead Implementer, <amendndozad@unitru.edu.pe>, ORCID: 0000-0002-0469-915X

1. INTRODUCCIÓN

Las empresas han sufrido modificaciones sustanciales al entrar en la época de la información, los diversos trabajos elaborados por las mismas producen perennemente agrupaciones de información acumuladas digitalmente. Ninguna empresa se ha mantenido indiferente a estos avances, en especial los de la ciencia de los datos. Por lo tanto, algún deterioro de los datos puede ser catastrófico; ella igual que no relacionar los datos de modo apropiado.

El Sistema de Gestión de Seguridad de la Información, o también llamado según sus iniciales SGSI, conforme ISO 27001, consiste en conservar la privacidad, completitud y existencia de los datos, tanto en los métodos comprendidos en la disposición ISO (Internacional Organization for Standardization) como en IEC (International Electrotechnical Commission). Ambos conforman el sistema técnico para la estandarización universal. Las entidades públicas socios de ISO e IEC colaboran en el progreso de las normas universales por medio de comisiones especialistas instauradas por la institución correspondiente para observar áreas específicas de la ocupación tecnológica. Las comisiones expertas de ISO e IEC cooperan con diferentes áreas de manera recíproca. Esta normativa se desarrolló para la instauración, aplicación, ejecución, vigilancia, verificación, conservación y mejoramiento de un SGSI en cualquier modelo de institución en soporte a las exigencias, finalidades, condiciones de protección, los procedimientos, los funcionarios, el volumen, los sistemas de apoyo y la estructura de las organizaciones. Esta normativa ha estado organizada procedimentalmente para acomodarse al prototipo "Planificar, Hacer, Verificar, Actuar" (Plan Do Check Act), el cual se utiliza para disponer en absoluto los procedimientos del SGSI. Esto se debe a que la normativa ISO 27001 labora sobre una perspectiva a procesos, una práctica minuciosa y precisa de la misma, necesita de un compendio de técnicas, completa y necesariamente instaurados, declarados, instruidos y corroborados. El adecuado boceto, establecimiento e intervención de un SGSI permite a la organización ejecutar más eficientemente sus tareas. [1]

La protección de los datos es un tema corporativo y, por eso, la expectativa adecuada para alcanzar un desempeño agradable consiste en usar esta tarea desde un planteamiento sistemático. este es utilizado por todas las organizaciones, no exclusivamente en un sentido de los procedimientos de los datos. Es elemental que el directivo de protección de los datos integre vastos conocimientos en un sistema de protección segura, así como los fundamentos y actividades imprescindibles con el fin de perfeccionar una táctica de protección de los datos, y un programa de acción para su puesta en marcha. A fin de certificar la salvaguarda de la información en las empresas, el SGSI es una de las habilidades que lograrían ejecutar. [2]

La garantía de los datos incluye un método práctico de dirección y protección de los datos, el cual debe mostrarse únicamente desde la perspectiva de su puesta en marcha, porque el SGSI es una fracción de la seguridad colectiva en las empresas. Bajo este entorno, el empleo de mejores ejercicios y ejemplares, como ISO, COBIT, ITIL, CMMI, PMBOK, OSSTMM, entre otros, ofrecen las directrices precisas para instaurar el entendimiento de la puesta en funcionamiento. Los inconvenientes de seguridad de los datos deben solucionarse a profundidad. Por lo tanto, la investigación de estos inconvenientes no debe ser fragmentada y restringida. [3]

La presente investigación tiene como finalidad primordial dar a entender los diferentes efectos que tiene para una organización la implementación de un método de protección de los datos bajo la normativa ISO 27001, para lo cual se ha elaborado una revisión sistemática de la literatura científica producida entre los años 2015 y 2021. A partir de lo expuesto, la pregunta de investigación es la siguiente: ¿cómo afecta la implementación de la seguridad de la información basado en las normas ISO/IEC 27001 en las organizaciones?

2. METODOLOGÍA

Se llevó a cabo una revisión sistemática apoyada en la acomodación y uso del método PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) [4].

Fundamentación de la Metodología

La utilización de la metodología PRISMA [4] tiene la capacidad de favorecer a cuantiosas agrupaciones de interés. Las difusiones enteras de exploraciones sistemáticas posibilitan a los leyentes

valorar la capacidad de los procedimientos y, por lo tanto, la confiabilidad de los descubrimientos. La muestra y síntesis de las particularidades de las investigaciones que ayudan a una simplificación autorizan a plantear consejos adecuados para la praxis o las políticas. La manifestación íntegra de todas las cláusulas de la exposición PRISMA 2020, además, permite la argumentación y reajuste de las exploraciones sistemáticas, y la incorporación de estas en revistas panorámicas, revistas de exploraciones metódicas (overviews) y en compendios de prácticas para que los investigadores puedan utilizar el esfuerzo realizado y obviar sacrificios insignificantes en sus averiguaciones.

Principios de Inclusión y de exclusión

- ***Principio de Inclusión***

✓ Escritos divulgados entre los años 2016 y 2021
✓ Escritos cuyos encabezados tengan las palabras clave "Seguridad de la Información", "Security of the information ", "empresa","company", "SGSI", "ISO/IEC 27001", y "Sistema de seguridad de la información"

- ***Principio de Exclusión***

✓ Investigaciones en diapositivas y ejemplares
✓ Lecturas grises que concuerdan con escritos no divulgados

De los escritos reiterados en varios archivos digitalizados, solo se eligió varios de ellos.

Proceso de Recolección de la información

El proceso de búsqueda y recolección de datos con ciertas palabras clave partió de la pregunta de investigación: "ISO/IEC 27001 (Information technology - Security techniques - Information security management systems - Requirements)", "Seguridad de Información", "Security of the information", "empresa", "company", "implementación", "implementation", "SGSI". Se determinó de modo más transparente la búsqueda de la lecturas científicas, y se crearon varias mezclas de las palabras clave anteriormente mencionadas: [("ISO/IEC 27001" e "implementación") y ("empresa") e ("implementation") y ("company") y ("Security of the information ") y ("Seguridad de la Información") y ("SGSI")]. Luego se definieron los soportes de datos en los que se hicieron las investigaciones en Alicia, Dialnet Plus, Redalyc y Scielo.

Los escritos y revistas científicas elegidos fueron llevados a un Excel, en el cual se examinó conforme a los siguientes principios de inclusión y exclusión. Se introdujeron escritos divulgados en motores de búsqueda científica y en almacenes académicos digitalizados, entre los años 2016 a 2021, que detallaron una perspectiva de impacto de los métodos de dirección de protección de los datos utilizando la normativa ISO 27001 en diferentes organizaciones. Así, esta designación parte de la siguiente manera según los impactos que ha tenido por el prestigio de la utilización de la normativa mencionada en la protección de los datos y en las extensiones de privacidad, completitud y recursos disponibles.

3. RESULTADOS

La investigación siguió los siguientes puntos. Se identificó 33 artículos de acuerdo con el título de la investigación de las diferentes bases de datos de artículos de investigación (Alicia, Dialnet Plus, Redalyc y Scielo), de los cuales, después de haberlos filtrado por los criterios de exclusión, se escogieron finalmente para la presente investigación 20 artículos para ser analizados a detalle. Cabe mencionar que la herramienta usada para la mayoría de las acciones de filtrado de los documentos fue la hoja de cálculo de Google.

La ubicación geográfica de los países a los que pertenecen las universidades o instituciones identificadas en el estudio evidencia que los artículos que tratan sobre de seguridad de la información en relación con la norma ISO 27001 son de interés global. No obstante, Colombia y Perú cuentan con el mayor número de instituciones referidas en los artículos, seguidas de Ecuador, mientras que en los demás países del primer mundo es inferior según se muestra en la figura 1.

De los 20 artículos seleccionados se resaltó el efecto de ejecución de un SGSI bajo la ISO 27001 en diversas organizaciones, ya sean locales como internacionales en siete fuentes. En la tabla 1, se muestran los 7 artículos

aplicativos identificados, que detallan el título, autor, años de publicación y el efecto que obtuvo la aplicación de un SGSI que sigue las directrices de la norma ISO 27001.

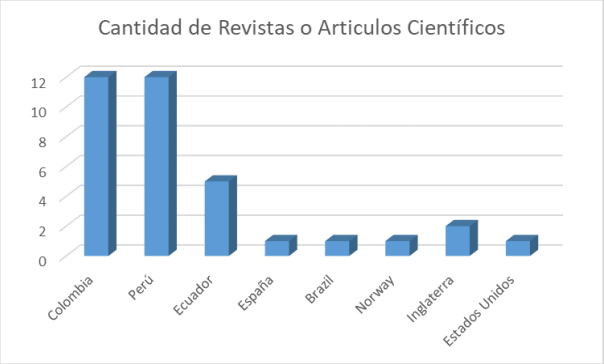

Figura 1. *Publicaciones diferenciadas por países*

N°	Título	Autor	Año	Efecto
1	Implementación de NTP ISO/IEC 27001 para la seguridad de información en el área de configuración y activos del ministerio de educación – sede CENTROMIN	Hugo Daniel Olaza Aliano	2017	-Mejoró la continuidad del negocio al gestionar de manera eficiente los riesgos

2	Seguridad de la información aplicando el ISO 27001:2013 para la oficina de registros y archivos académicos de la universidad nacional del callao 2017	Irving José Valverde Reyes	2018	-Redujo los riesgos significativamente con respecto al manejo de la información generada por el área de recursos
3	Mejora de los procesos de tecnologías de la información aplicando COBIT 5.0 y la norma técnica peruana NTP-ISO 27001: 2014. Caso: autoridad autónoma de majes	Javier Fernando Angulo Osorio	2018	-Aumentó de la eficiencia de los servicios informáticos de la organización -Aumentó del grado de preservación de la Información de la organización -Mejoró soporte es las tareas habituales de la información -Aumentó los conocimientos de los procesos por parte de los colaboradores de la entidad -Aumentó la comprensión de las políticas de seguridad de la organización
4	Plan de mejora de la seguridad de la información del seguro social de salud – ESSALUD aplicando estándar ISO/IEC 27001	Luis Alejandro Poma Rosales	2019	-Redujo el índice de accesos no autorizados, disminuyendo el riesgo de filtraciones de los datos de la organización -Aumentó el tiempo de disposición de los datos de la organización -Aumentó el índice de operatividad del servicio -Aumentó el índice de información correcta en los Backups
5	Sistema de gestión de seguridad de información (sgsi) basado en la norma iso/iec27001 para mejorar la seguridad del área de operaciones y tecnología de global bpo center allus chiclayo - 2015	Rojas Viera Cinthia Katherine, Zavaleta Verona Tefhany Lisseth.	2019	-Redujo los niveles de riegos de los activos de la organización -Diferencia de la competencia a nivel local y nacional -Redujo el riesgo de pérdida o robo de la información -Minimizó las discontinuidades en las actividades de la empresa
6	Aplicación de iso 27001 y su influencia en la seguridad de la información de una empresa privada peruana	Liset Sulay Rodriguez Baca Carlos Francisco Cruzado Puente De La Vega Carolina Mejía Corredor Mitchell Alberto Alarcón Diaz	2020	-Redujo el riesgo del esparcimiento no aprobado de la información empresarial -Redujo las el número de modificaciones no permitidas de la información empresarial
7	Sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo de COOPSOL consultoría, 2019	Carlos Alberto Huerta Agurto	2020	-Se logró aumentar la cantidad de controles empleados en el transcurso de la gestión de los riesgos. -Se redujo la cantidad de peligro en el proceso de gestión de COOPSOL Consultoría.

Tabla 1. *Impactos identificados en las publicaciones consultadas*

En el análisis de estos siete artículos se muestra cómo los sistemas de seguridad de la información han aumentado la confidencialidad, disponibilidad e integridad de los datos de las respectivas organizaciones en las cuales se desarrolló el estudio. por ejemplo, en el Hospital Víctor Lazarte Echegaray de la Red Asistencial La Libertad–EsSalud, al incorporar este sistema, aumentó la confidencialidad en un 17.59%, disponibilidad en un 30.51% y la integridad en un 14.66% [5]. Según Valverde, se determinan los peligros, amenazas y vulnerabilidades en los procesos al utilizar un sistema de seguridad de la información bajo la norma ISO 27001

[6]. Por otro lado, se reconoció que la utilización de un SGSI bajo ISO 27001 fue beneficioso para la organización, ya que aumentó la seguridad en los sistemas de información, lo cual ayudó en la mejora constante en cada escalón de la auditoría interna, lo que a su vez incrementó la confianza y mejoró la imagen corporativa [7].

4. DISCUSIONES Y CONCLUSIONES

Discusiones

En el siguiente apartado se muestran los diferentes impactos que obtuvieron las organizaciones al emplear un SGSI siguiendo las directrices de la norma ISO 27001.

Olaza afirma que el empleo de la ISO 27001 aumentó la seguridad de los datos en el área de Configuración y Activos del Ministerio de Educación, Sede Centromin, con una confidencialidad del 95%, lo cual aumentó el grado de seguridad de dicha organización, además de reducir el promedio de información divulgada en un 72.5%, al igual que el promedio de accesos no autorizados en un 85.4% y, por último, incrementó el porcentaje de aptitud del sistema para ser utilizado por el usuario en un 39.7% , lo cual tuvo un impacto positivo en la continuidad de los procesos de la organización [8]. Valverde también manifiesta resultados similares. En su investigación, expresa que la confidencialidad de la información de la Oficina de Registros y Archivos Académicos aumentó de 67% a 97%, asimismo la disponibilidad pasó de un 28% a un 95% y, por último, la integridad, que es el impacto con mayor diferencia, se incrementó de un 17% a un 95% [6]. Poma también llega a la misma conclusión, de que la implementación de un SGSI bajo ISO 27001 aumenta de la seguridad de la información (Disponibilidad ↑30.51%, Confidencialidad ↑17.59% e Integridad ↑14.66%). [5]

Por otro lado, Angulo explica que se mejoraron los procesos de tecnologías de la información. Además, a diferencia de los dos autores mencionados con anterioridad, señala dos efectos importantes que son el mayor conocimiento de los procesos por parte de los miembros de la organización y el mayor conocimiento de los estándares de seguridad que la organización maneja internamente, lo que refuerza la eficiencia de los servicios informáticos de la organización [9].

Pedraza afirma que la utilización de los sistemas de gestión de la protección de los datos establece los peligros al interior de una compañía, y genera un efecto en cascada, ya que influye notoriamente en apartados como la disponibilidad, la confidencialidad e integridad de los datos de las compañías, ya que redujo el riesgo de la divulgación no autorizada de la información empresarial y de modificaciones no permitidas de la información empresarial. Esto, sea a su vez, impacta en el crecimiento y sostenibilidad de la empresa [7]. En ese sentido, coincide con Huerta, que concluye que el sistema de gestión de la protección de la información afecta positivamente pues disminuye los peligros en el transcurso de la gestión del riesgo de Coopsol Consultoría [10].

Por último, Macedo y Castillo plantean otro impacto positivo en las organizaciones muy diferente a las expuestas en las demás lecturas, ya que considera que la implementación del SGSI actúa en favor de la entidad. Esto se debe a que produce una mejora en la seguridad en los sistemas de información y ayuda a obtener una mejora constante en cada escalón de la auditoría interna, lo cual aumenta la credulidad y mejora de imagen corporativo. Sin embargo, cabe recalcar que este trabajo no es un trabajo aplicativo, así que, los efectos no pueden ser contrastados en su totalidad [11]. Al respecto, Rojas y Zavaleta (2019) publicaron un trabajo aplicativo en el cual afirman que la aplicación de un SGSI normado por la ISO 27001 influye positivamente en la diferenciación de la competencia a nivel local y nacional con respecto a la ornamentación [12].

Conclusiones

En la presente revisión sistemática sobre las características de la administración de seguridad de la información bajo las directrices de la ISO/IEC 27001 en las organizaciones, se logró identificar los efectos de todos los activos de información, riesgos de seguridad y establecer los controles para gestionar las amenazas, que generan, a su vez, un aumento en la seguridad que sienten los clientes, proveedores o interesados en sus servicios.

Por eso, concluimos que los efectos de la implementación de SGSI que siguen las directrices de la ISO 27001 trae consigo los siguientes afectos a las empresas:

- Mejora la continuidad del negocio
- Reduce los riesgos significativamente con respecto a la gestión de la información como modificaciones no autorizadas de la información empresarial, divulgación no autorizada de la información empresarial, accesos no autorizados, pérdida o robo de datos empresariales
- Reducción de los valores de riegos de los activos de la organización
- Aumento de la eficiencia de los servicios informáticos de la organización
- Mejoramiento del soporte es las tareas habituales de la información
- Aumento del tiempo de disposición de la información
- Diferenciación de la competencia a nivel local y nacional

Finalmente, la revisión sistemática reveló la realidad sobre la gestión de la protección de los datos en las organizaciones, dado que las redes corporativas pueden sufrir ataques desde cualquier computador ubicado en cualquier lugar remoto con acceso a internet. Además, señala el impacto que tiene la utilización de un SGSI regido por la ISO 27001 como el aumento de la confidencialidad, disponibilidad e integridad de los datos de la organización, así como la mejora de la imagen de la misma.

REFERENCIAS BIBLIOGRÁFICAS:

[1] A. R. Mantilla Guerra, «Gestión de seguridad de la información con la norma ISO 27001:2013,» *ESPACIOS*, vol. 39, nº 18, p. 5, 2018.

[2] H. Laksono y Y. Supriyadi, «Design and implementation information security governance using Analytic Network Process and cobit 5 for Information Security a case study of unit XYZ,» de *2015 International Conference on Information Technology Systems and Innovation (ICITSI)*, 2015.

[3] A. Budi Setiawan, A. Syamsudin y A. Sasongko Sastrosubroto, «Information security governance on national cyber physical systems,» de *2016 International Conference on Information Technology Systems and Innovation (ICITSI)*, 2016.

[4] J. Yepez Nuñez, G. Urrútia, M. Romero García y S. Alonso Fernandéz, «Declaración PRISMA 2020: una guía actualizada para la publicación de revisiones sistemáticas,» *Revista Española de Cardiología*, vol. 74, pp. 790-799, 2021.

[5] L. A. Poma Rosales, «Plan de mejora de la seguridad de la información del Seguro Social de Salud – EsSalud aplicando estándar ISO/IEC 27001,» Trujillo, 2019.

[6] I. Valverde Reyes, «Seguridad de la información aplicando el ISO 27001:2013 para la oficina de registros y archivos académicos de la Universidad Nacional Del Callao 2017,» Callao, 2017.

[7] G. Pedraza Rodríguez, «Plan de implementación de un sistema de gestión de seguridad de la información en una entidad del sector público basado en la NTC ISO 27001:2013,» Bogotá, 2017.

[8] H. Olaza Aliano, «Implementación de NTP ISO/IEC 27001 para la Seguridad de Información en el Área de Configuración y Activos del Ministerio de Educación – Sede Centromin,» Lima, 2017.

[9] J. Angulo Osorio, «Mejora de los Procesos de Tecnologías de la Información Aplicando Cobit 5.0 y la Norma Técnica Peruana Ntp-Iso 27001: 2014. Caso: Autoridad Autónoma de Majes,» Arequipa, 2018.

[10] C. Huerta Agurto, «Sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo de Coopsol Consultoría, 2019,» Lima, 2020.

[11] E. Javier Macedo y H. Luna Castillo, «Propuesta de guía metodológica basada en ISO/IEC 27001:2013 y NTP ISO/IEC 27001:2014 en la seguridad de la información en la Municipalidad Provincial de Recuay - 2015,» Huaraz, 2019.

[12] C. Rojas Viera y T. Zavaleta Verona, «Sistema de Gestión de Seguridad de Información (SGSI) Basado en la Norma ISO/IEC27001 para mejorar la Seguridad del Área de Operaciones y Tecnología de Global BPO Center Allus Chiclayo - 2015,» Chiclayo, 2015.