Editada por la Dirección de Investigación, UNIBE, Quito
QUALITAS revista científica
LATINDEX; ISSN-L: 1390-656 / ISSN: 1390-6569 / ISSN-(En línea): 2661-6610

EVALUACIÓN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LOS SISTEMAS DE INFORMACIÓN GERENCIAL COMO HERRAMIENTA DE COMPETITIVIDAD EN EMPRESAS DE SERVICIOS DE ENSAYOS NO DESTRUCTIVOS EN LA CIUDAD DE LIMA - PERÚ

EVALUATION OF INFORMATION SECURITY MANAGEMENT IN MANAGEMENT INFORMATION SYSTEMS AS A TOOL OF COMPETITIVENESS IN COMPANIES OF NON-DESTRUCTIVE TESTING SERVICES IN THE CITY OF LIMA – PERU

Juan J. Lugo Marín*, Hector E. Carrasquero* & Jesús O. Gómez Rivero**

* Departamento de Gerencia. Universidad Nacional Experimental "Francisco de Miranda". Prolongación Av. Táchira, Edificio El Sabino. Punto Fijo – Estado Falcón, Venezuela
** Dirección de Investigación, Universidad Iberoamericana del Ecuador, Quito-Ecuador.

Autor corresponsal: juanlugomarín@hotmail.com

Manuscrito recibido el 25 de mayo de 2020.
Aceptado para publicación, tras proceso de revisión, el 12 de junio de 2020.

Resumen

El objetivo del presente artículo es llevar a cabo una evaluación de la manera como se gestiona la seguridad de la información tomando como base la Norma internacional ISO 27001:2013 en los sistemas de información gerencial (SIG) en un grupo de empresas de servicios de ensayos no destructivos (END) que operan en Lima-Perú. El estudio fue desarrollado en base a una investigación documental y de campo de tipo descriptiva, en la que se integra y armoniza el enfoque cualitativo y cuantitativo de investigación. En lo que respecta a las técnicas de recolección de información, se emplearon: la observación directa, el análisis de fuentes documentales y el cuestionario. Entre los resultados más destacados se tiene que el análisis de la información recolectada permitió esquematizar el proceso de concepción e implementación de un sistema de información gerencial, para luego a partir de los lineamientos prescritos en la norma internacional ISO 27001 determinar el nivel de cumplimiento respecto a la seguridad de la información, para finalmente formular algunas reflexiones teóricas en relación a la vinculación de la seguridad de la información en los sistemas de información gerencial en el grupo de empresas seleccionadas. Como conclusión relevante se obtuvo que aunque las empresas participantes en la investigación han hecho avances significativos en la adopción de sus sistemas de información gerencial no ha sido lo mismo con la gestión de la seguridad de la información la cual se considera aún débil en estas empresas, lo que las hacen particularmente vulnerables.

Palabras Claves: sistema de información gerencial, seguridad de la información, ISO 27001.

Abstract

The objetive of this article is to carry out an evaluation of the way in which information security is managed based on the International Standard ISO 27001: 2013 in management information systems in a group of testing services companies. operating in Lima-Peru. The study was developed based on a descriptive and documentary field research, in which the qualitative and quantitative research approach is integrated and harmonized.

Editada por la Dirección de Investigación, UNIBE, Quito
QUALITAS revista científica
LATINDEX; ISSN-L: 1390-656 / ISSN: 1390-6569 / ISSN-(En línea): 2661-6610

Regarding information collection techniques include: direct observation, analysis of documentary sources and the questionnaire. Among the most outstanding results is that the analysis of the information collected allowed to outline the process of conception and implementation of a management information system, and then from the guidelines prescribed in the international standard ISO 27001 determine the level of compliance with respect to information security, to finally formulate some theoretical reflections in relation to the linkage of information security in management information systems in the group of selected companies. As a relevant conclusion, it was obtained that although the companies participating in the research have made significant advances in the adoption of their management information systems, it has not been the same with the management of information security, which is still considered weak in these companies. which makes them particularly vulnerable.

Key Words: management information system, information security, ISO 27001.

1. INTRODUCCIÓN

Hoy día en pleno siglo XXI las distintas organizaciones, independientemente de su naturaleza o tamaño, centran sus esfuerzos en mantenerse y ser exitosas en un mercado global caracterizado por una fuerte competencia. Las distintas organizaciones para lograr ser competitivas, hacen esfuerzos considerables en la adopción de diversos enfoques gerenciales, en muchos de los cuales resulta un factor clave del éxito el contar con una infraestructura tecnológica que facilite la interacción continua con su contexto de manera adecuada, facilitando la promoción, colocación y/o prestación de sus productos o servicios. En ese sentido, los sistemas de información gerencial juegan un rol preponderante que facilitan los procesos de captación, procesamiento y divulgación de la información tanto al ámbito externo de la organización como hacia los procesos internos de la misma, permitiendo de esta manera dinamizar de una manera eficaz los diversos canales de control dentro de las operaciones y actividades empresariales, facilitando el logro de políticas y objetivos, así como la retroalimentación de elementos sensibles para el éxito organizacional. No obstante, hoy día resulta imperioso integrar estos enfoques de sistemas de información con lo que es su seguridad, existiendo estándares internacionales para establecer sistemas de gestión de seguridad de la información como lo es la norma ISO 27001.

Cuando se habla de sistemas de información gerencial (SIG) resulta ineludible abordar el concepto de información el cual se ha relacionado con el concepto de datos e incluso con el de conocimiento (Nonaka & Byosiere, 2010). Se destaca que muchos autores incluyen el concepto de dato como elemento de entrada para la información, es decir como materia prima o punto de partida de la información, y como

Editada por la Dirección de Investigación, UNIBE, Quito
QUALITAS revista científica
LATINDEX; ISSN-L: 1390-656 / ISSN: 1390-6569 / ISSN-(En línea): 2661-6610

producto acabado (Davis & Olson, 2016). Es por ello, que se suele considerar a la información como un elemento protagónico en el proceso de toma de decisiones (Arteaga, Cardenas, & Dávila, 2016) el cual es fundamental para generar procesos de comunicación a diversos niveles (Gauchi, 2012). Conocimiento e información constituye un todo indivisible que se erigen como recursos estratégicos y fuente de transformación de las organizaciones y la sociedad en general (Larrocha, 2017). Entonces los datos pueden emplearse para ser procesados para luego llegar a la generación de información, la cual va a soportar el proceso de toma de decisiones en diferentes niveles, permitiendo su contextualización y clasificación, a partir del análisis sistemático que luego más tarde es categorizado y que sustenta la interpretación lo que va hacer posible su empleo posterior y que es insumo fundamental al momento de decidir (Bagad, 2015).

Un SIG es la resultante de un proceso estructurado de colección y procesamiento de datos de acuerdo a las necesidades específicas de una organización para luego clasificar, almacenar y distribuir de una manera selectiva la información necesaria para la operación organizacional, así como las actividades de dirección y estrategia apoyando el proceso de toma de decisiones gerenciales en función de las estrategias empresariales (Andreau, Ricart, & Valor, 2016), lo cual complementa el control estratégico de la organización y el logro de su visión y misión (Hernández, 2011) . También se puede relacionar los sistemas de información como el conjunto de personas, datos, información, así como las herramientas para procesar y almacenar información en el ámbito de una organización haciendo uso de las tecnologías de información y de comunicación (Heeks, 2007)

Dada la importancia estratégica que reviste hoy día la información y los sistemas sobre los cuales estos se soporta, surge la necesidad de integrar a estos sistemas un nuevo elemento: la seguridad de la información, la misma se relaciona con un sistema de ideas básicas relacionadas con la protección de la información en sistemas de procesamiento modernos, proporcionando una visión holística de la naturaleza del problema de protección, las leyes de su desarrollo y vínculos significativos con otras ramas del conocimiento, formadas y desarrolladas en base a experiencia práctica, tareas de protección y definición de las pautas básicas en la dirección de mejorar la práctica de protección de la información (Syreyshchikova, Pimenov, Mikolajczyk, & Moldovan, 2019)

Para apoyar lo anterior se ha desarrollado la norma ISO 27001 la cual contempla los elementos a considerar en un Sistema de Gestión de Seguridad de la Información (SGSI) partiendo del hecho de que

la información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. El hecho de no proteger adecuadamente este elemento puede tener consecuencias operativas, financieras y legales. El reto que la mayoría de negocios afronta es el de proporcionar una adecuada protección. Particularmente, cómo asegurar que han identificado los riesgos a los que están expuestos y cómo gestionarlos de forma proporcionada, sostenible y efectiva. Más allá de la forma como la información es almacenada o trasmitida los SGSI, según la norma ISO 27001, se basan en la garantía y preservación del carácter confidencial de la misma, así como su integridad y disponibilidad, incluyendo de igual manera los sistemas relacionados con su tratamiento.

La aplicación práctica de los SIG ha sido muy amplio en el sector industrial tanto en empresas productoras de bienes tangibles como de servicios. En el sector de servicios llama la atención las empresas que se dedican a los trabajos de inspección y ensayos no destructivos (END) las cuales manejan información sensible en la ejecución de proyectos, mantenimientos correctivos, preventivos, rutinarios a instalaciones industriales, la cual debe ser gestionada ágilmente por parte de quienes toman decisiones, al mismo tiempo que debe manejarse bajo principios de seguridad que garanticen su confidencialidad, integridad y disponibilidad. En la ciudad de Lima – Perú, existe un importante número de empresas dedicadas a este sector industrial las cuales han llevado a cabo esfuerzos considerables en la implementación de sus SIG. No obstante aun cuando existe la visión generalizada por parte de los ejecutivos, sobre las ventajas de contar con este tipo de sistemas, en la práctica se presenta la inquietud generalizada respecto a la vulnerabilidad de los mismos ante lo que se conoce como seguridad de la información.

La mayoría de las empresas del sector de servicios de Ensayos No Destructivos disponen, gestionan y tienen acceso a información confidencial no solo de estas organizaciones y sus clientes sino que para otros grupos de interés como son proveedores, subcontratistas y clientes. Es por lo anterior que surge el interés de llevar a cabo esta investigación, más cuando es palpable la necesidad de proporcionar una adecuada protección. Particularmente, cómo asegurar que han identificado los riesgos a los que están expuestos y cómo gestionarlos de forma proporcionada, sostenible y efectiva. En ese sentido la Norma Internacional ISO 27001: 2013 proporciona un marco robusto para proteger la información que se puede adaptar a organizaciones de todo tipo y tamaño. Es por esta razón que las organizaciones más expuestas a los riesgos relacionados con la seguridad de la información eligen cada vez más implementar un SGSI

que cumpla con la norma ISO 27001. De allí la importancia de evaluar los sistemas de información gerencial de un grupo de empresas del sector servicios de ensayos no destructivos en Lima – Perú con la mencionada norma, a los fines de contribuir a su éxito y permanencia en el tiempo. Los objetivos trazados en la presente investigación son los siguientes:

Objetivo General

Evaluar la gestión de la seguridad de la información en base a la Norma ISO 27001:2013 en los sistemas de información gerencial de un grupo de empresas de servicios de Ensayos No Destructivos que operan en la ciudad de Lima - Perú.

Objetivos específicos

- Describir la implementación del sistema de información gerencial en las empresas seleccionadas.
- Diagnosticar el sistema de información implementado en base a la Norma ISO 27001: 2013.
- Analizar la relación de interdependencia que existe entre la gestión de seguridad de la información y la implementación de SIG en el ámbito de las empresas de servicios objeto de este estudio.

2. MÉTODOS

La presente investigación armoniza e integra los enfoques cualitativos y cuantitativos de investigación para su desarrollo. De igual manera, para el logro de los objetivos establecidos, el presente estudio plantea una metodología de investigación de tipo descriptiva y documental con un diseño de campo. En base a Hernández Sampieri (2014) se dice que es una investigación documental ya que se revisaron documentos científicos y técnicos relacionados al objeto de la investigación así mismo es de campo puesto que se consultó directamente sobre los actores de las empresas objeto de estudio sobre el proceso de formalización y adopción de sistemas de información gerencial considerando para ello los requisitos de la Norma ISO 27001.

En este estudio se combina el análisis crítico, el cotejo y la integración de perspectivas expuestas por diversos autores acerca del tema planteado. En relación con el enfoque metodológico, la investigación combinó diversos enfoques: Descriptivo porque se estudiaron los aspectos teóricos relevantes en torno a

las dimensiones que orientan la presente investigación (Saez López, 2017). Lo cual permitió a partir de los planteamientos desarrollados caracterizar lo que son los sistemas de información gerencial para las empresas de servicios de ensayos no destructivos; y para luego llevar a cabo el diagnóstico del nivel de cumplimiento de los requisitos de la Norma ISO 27001 en los sistemas de información gerencial desarrollados por las empresas objeto de estudio.

La población del estudio viene dado por las empresas del sector de ensayos no destructivos (END) que hayan implementado sistemas de información gerencial y que operan en la ciudad de Lima Perú. La muestra, según Hernández (2014), representa el subgrupo de la población del cual se recolectarán los datos. En ese sentido, se llevó a cabo un muestreo intencionado, considerando dos aspectos claves: i) empresas de ensayos no destructivos que hayan implementado un sistema de información gerencial y ii) empresas que estén dispuestas a compartir su información de experiencias y vivencias en la implementación de su SIG. Por muestreo intencionado se entiende el tipo de muestreo que se produce cuando los elementos seleccionados para conformar la muestra son elegidos en base a los criterios establecidos por el investigador Saez López (2017).

Para la evaluación de la gestión de la seguridad de la información en la muestra de empresas seleccionadas se utilizó una lista de verificación, en base a cada uno de los siete requisitos o cláusulas de la Norma ISO 27001: 2013, a saber: i) contexto de la organización, ii) liderazgo, iii) planificación, iv) soporte, v) operación, vi) evaluación del desempeño y vii) mejora. El instrumento constó de sesenta ítems cuyas convenciones para la evaluación fueron: i) cumple, ii) no cumple y iii) no aplica. El instrumento fue validado por tres expertos en el área de gestión de seguridad de la información. Los expertos consideraron aspectos como: i) redacción, referido a la forma como están constituidos cada ítem desarrollado y ii) pertinencia, referido al grado en que cada item considerado guarda relación con el requisito de la norma ISO 27001: 2013.

3. RESULTADOS Y DISCUSIÓN

Como punto de partida para el presente estudio se seleccionó un grupo de cuatro empresas de Servicios en el área de Ensayos No Destructivos (END) establecidas en Lima – Perú, desde donde despliegan operaciones para las diversas localidades que demandan los servicios ofrecidos. Respetando el principio de confidencialidad de la información, asumido con las empresas objeto de estudio, los resultados de la

investigación se presentarán de manera consolidada. Se destacan los siguientes aspectos del grupo de empresas seleccionadas:

- Todas son privadas y tienen más de 5 años de operación.
- Sus clientes están tanto en el sector público y privado, ubicándose principalmente en los siguientes sectores: gasífero, petróleo, minero y terminales marítimos.
- Los principales servicios ofrecidos por estas empresas, se ubican en el área de Ensayos No Destructivos e incluyen: radiografía industrial, ultrasonido convencional, ultrasonido phased array, partículas magnéticas, líquidos penetrantes, identificación positiva de materiales.
- Una de las empresas cuenta con un Sistema de gestión de la calidad ISO 9001: 2015 certificado. Las otras tres señalaron que lo tienen implementado más no lo tienen certificado.
- Dos de las empresas estudiadas tienen implementada la norma ISO 17020 y están en vía de acreditación.
- Las cuatro empresas que formaron parte de la investigación han implementado SisteSIG y el mismo es objeto de mantenimiento y seguimiento continuo por parte de la alta dirección.

3.1 Implementación del sistema de información gerencial en la empresa seleccionada.

Cada una de las empresas que formaron parte de la investigación han implementado un sistema de información gerencial, cada una tiene su propio proceso de instauración, sin embargo, producto de la investigación se lograron identificar fases o etapas comunes que se pueden definir como claves para la implementación de un SGI. Estas etapas aparecen identificadas en la Figura No. 1 y se explican a continuación.

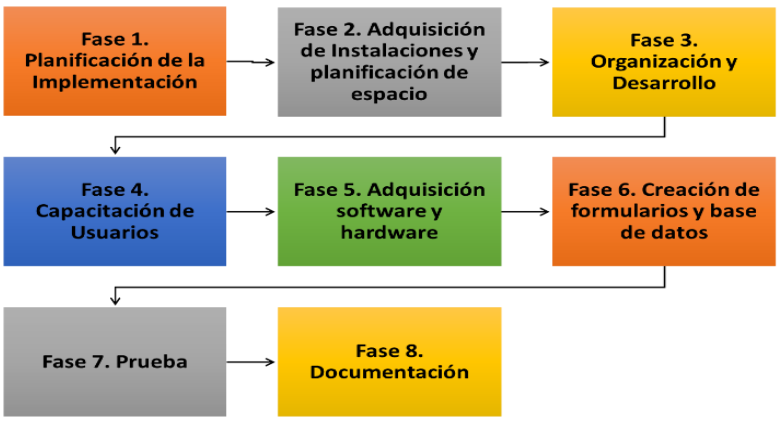

Fig. 1 Proceso de implementación de Sistema de Información Gerencial.

Fase 1 (Planificación de la implementación): como punto inicial en la implementación de un sistema de información gerencial se identificó la fase de planificar, esta fase representa una actividad previa a la implementación. En la planificación se determinan y formulan las diversas actividades que son necesarios llevar a cabo para la implementación del sistema de información gerencial.

Fase 2 (Adquisición de instalaciones y planificación del espacio): dado que en las empresas consideradas en la investigación los sistemas de información gerencial fueron desarrollados por primera vez, es decir no había ningún sistema existente con anterioridad se hizo necesaria la adquisición de instalaciones de oficina, sala de informática y recursos tecnológicos, entre otros.

Fase 3 (Organización y desarrollo de procedimientos): en esta fase las empresas consultadas llevaron a cabo las contrataciones del personal requerido. De igual manera se identificaron las tareas a llevar a cabo por los distintos usuarios, identificando barreras y posibles resistencias, en esta fase se desarrollaron los protocolos procedimentales de los usuarios finales.

Fase 4 (Capacitación de usuarios): se pudo constatar como parte de la investigación, que la capacitación del usuario es una actividad importante de un SIG, para asegurarse que los usuarios finales sean capacitados para operar un nuevo sistema o como deberían actuar en caso que el sistema fallara. Es importante destacar que esta fase de capacitación, es un proceso continuo durante todo el la implementación del SIG, por lo que no se pretende situarse la misma como un paso o etapa rígida durante todo el proceso global.

Fase 5 (Adquisición de hardware y software): el proceso de adquisición de hardware y software comienza una vez que las especificaciones del diseño del sistema han terminado. En esta fase se incluye la preparación del sitio de trabajo donde va a estar el hardware, distribución de la sala de informática, aires acondicionados y las conexiones eléctricas que serán requeridas.

Fase 6 (Creación de formularios y de base de datos): esta fase se relaciona en la elaboración de los diversos formularios requeridos por el SIG, incluyendo los necesarios para la entrada y la salida de datos y la implementación global del sistema de información, teniendo en cuenta que los formularios se generan de acuerdo a la totalidad proceso.

Editada por la Dirección de Investigación, UNIBE, Quito
QUALITAS revista científica
LATINDEX; ISSN-L: 1390-656 / ISSN: 1390-6569 / ISSN-(En línea): 2661-6610

Fase 7 (Pruebas): esta fase de prueba del sistema implica probar dispositivos de hardware, software y depuración de programas informáticos y pruebas de procesamiento operacionales.

Fase 8 (Documentación): el desarrollo de la documentación es una parte importante del proceso de implementación de un sistema de información gerencial. En el desarrollo de la documentación se incluye la elaboración de manuales, muestra de pantalla, formularios e informes entre otros.

3.2 Diagnóstico según la norma ISO 27001.

Una vez caracterizados los Sistemas de Información Gerencial implementados por las empresas objeto de estudio el siguiente paso consistió en hacer una evaluación del nivel de cumplimiento de los requisitos establecidos en la Norma ISO 27001, los resultados consolidados se presentan en la Tabla No. 1 y en el Gráfico 1, en estos gráficos destaca un nivel de cumplimiento bastante bajo, cuyo promedio general consolidado se ubica aproximadamente en el 39%, existiendo una brecha significativamente amplia para llegar al nivel de cumplimiento requerido que es el 100%. De lo anterior se evidencia un nivel incipiente en lo que respecta a la adopción de un sistema de gestión de seguridad de la información entre las empresas que participaron en el estudio.

Tabla 2: Nivel de cumplimiento ISO 27001: 2013

Clausula	Descripción del Requisito	% de Cumplimiento
4	Contexto de la Organización	47
5	Liderazgo	48
6	Planificación	54
7	Soporte	53
8	Operación	50
9	Evaluación del desempeño	33
10	Mejora	33

Editada por la Dirección de Investigación, UNIBE, Quito
QUALITAS revista científica
LATINDEX; ISSN-L: 1390-656 / ISSN: 1390-6569 / ISSN-(En línea): 2661-6610

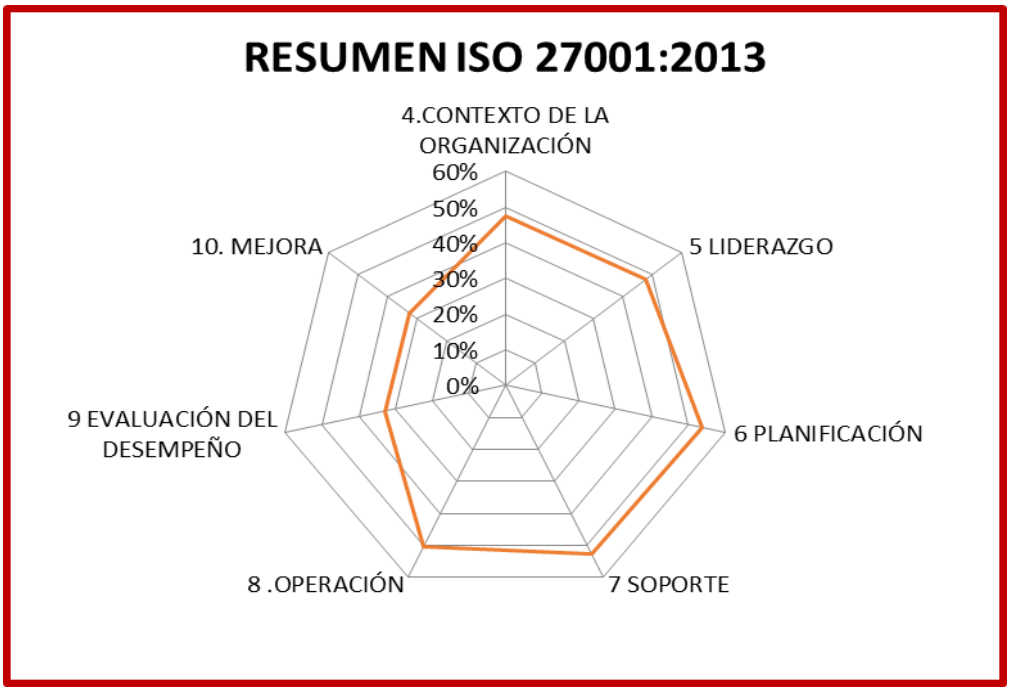

Gráfico 1. Resumen de cumplimiento ISO 27001: 2013

El estudio se hizo en base al nivel de cumplimiento de los cláusulas y sub cláusulas especificadas en la Norma ISO 27001:2013 en los sistemas de información gerencial de las empresas consideradas en el estudio, teniendo en cuenta el deber ser para los sistemas de gestión de seguridad de la información. El diagnóstico se llevó a cabo para cada empresa obteniéndose el porcentaje de cumplimiento individual, posteriormente se procedió a promediar los porcentajes de cumplimiento entre las cuatros organizaciones participantes en la investigación, destacando los siguientes aspectos:

Cláusula 4 Contexto de la organización: un análisis cuidadoso del entorno en el que opera la organización es fundamental para identificar los riesgos inherentes a la seguridad de sus activos de información. El análisis es la base que le permitirá evaluar qué procesos necesita considerar agregar o fortalecer para construir un SGSI efectivo. Este requisito comprendió la evaluación de: los requerimientos de las partes interesadas pertinentes, el alcance del sistema de gestión de seguridad de la información así como el enfoque de procesos. El nivel de cumplimiento promedio del grupo de empresas que conformaron el estudio fue de 47%.

Cláusula 5 Liderazgo: el liderazgo significa una participación activa en la dirección del SGSI, promover su implementación y garantizar la disponibilidad de recursos apropiados. Esto incluye: i) Asegurar que

los objetivos del SGSI sean claros y estén alineados con la estrategia general; ii) Claridad sobre las responsabilidades; iii) Que el pensamiento basado en el riesgo está en el corazón de toda toma de decisiones; y iv) Hay una comunicación clara de esta información a todas las personas dentro del alcance del SGSI. La ISO 27001 otorga gran importancia a la participación activa de la gerencia en el SGSI, basándose en el supuesto de que es crucial para garantizar la implementación y el mantenimiento efectivo de un SGSI efectivo y el mismo se relaciona con la responsabilidad de la alta dirección en relación al Sistema de Gestión de Seguridad de la Información. La evaluación llevada a cabo tuvo aspectos como: cumplimiento de política y los objetivos del SGSI, contar con los recursos requeridos, determinar los roles y las responsabilidades del personal de la organización. El porcentaje promedio de cumplimiento de este requisito también fue bajo reflejado en un 48%.

Cláusula 6 Planificación: la Norma ISO 27001 es una herramienta de gestión de riesgos que guía a una organización en la identificación de riesgos de seguridad de la información. Como tal, el propósito subyacente del requisito de Planificación en un SGSI es: i) Identificar los riesgos estratégicamente importantes, obvios y ocultos pero peligrosos; ii) Asegurarse de que las actividades y los procesos operativos diarios de una organización estén diseñados, dirigidos y tengan recursos para gestionar inherentemente esos riesgos; y iii) Responder y se adaptarse automáticamente a los cambios para hacer frente a los nuevos riesgos y reducir continuamente la exposición a los mismos. Tener un plan de acción detallado que esté alineado, actualizado y respaldado por revisiones y controles regulares es crucial y proporciona evidencia para el auditor de una planificación del sistema claramente definida. el cual está enfocado por un lado a la gestión de riesgos en el marco del sistema de seguridad de la información y por otro lado a definir los objetivos de seguridad de la información, los mismos debes ser claros y deben contar con planes específicos para su logro. El porcentaje promedio de cumplimiento de este requisito fue del 54%.

Cláusula 7 Soporte: la cláusula 7 se refiere a los recursos. Esto se aplica a las personas, infraestructura, medioambiente, recursos físicos, materiales, herramientas, entre otros. También existe un enfoque renovado en el conocimiento como un recurso importante dentro de su organización. Cuando se planifican los objetivos, una consideración importante será la capacidad actual y la capacidad de sus recursos, así como aquellos recursos de proveedores/socios externos, estando estos orientados a establecer, implementar y mejorar el Sistema de Gestión de Seguridad de la Información según la norma

Editada por la Dirección de Investigación, UNIBE, Quito
QUALITAS revista científica
LATINDEX; ISSN-L: 1390-656 / ISSN: 1390-6569 / ISSN-(En línea): 2661-6610

ISO 27001, en el que se incluye: Recursos, Personal competente, Conciencia y comunicación de las partes interesadas, información documentada y la conservación de la documentación correspondiente al Sistema de Gestión de Seguridad de la Información. Se obtuvo en este requisito un nivel de cumplimiento promedio del 53%.

Cláusula 8 Operación: esta cláusula viene a ser el corazón de la norma y está relacionado con el funcionamiento del Sistema de Gestión de Seguridad de la Información ISO 27001, las expectativas de la dirección y su retroalimentación, además de cumplir con lo que establece la referida norma. Relacionado con este requisito se tiene la planificación y control las operaciones y los requisitos de seguridad. Los activos, las vulnerabilidades y las amenazas ya no son la base de la evaluación de riesgos, solo es necesario para identificar los riesgos asociados con la confidencialidad, integridad y disponibilidad. Se obtuvo en este requisito un nivel de cumplimiento promedio del 50%.

Cláusula 9 Evaluación del desempeño: esta cláusula constituye la base para la identificación y medición de la eficiencia y el desempeño del sistema de gestión en base a los procesos de evaluación y seguimiento, auditoría interna y revisión por la dirección. Se obtuvo un nivel de cumplimiento promedio bastante bajo del 33%

Cláusula 10 Mejora del SGSI: el objetivo de la implementación del SGSI debe ser reducir la probabilidad de que ocurran eventos de seguridad de la información, así como su impacto. Ningún SGSI es perfecto, sin embargo, dichos sistemas de gestión mejoran con el tiempo y aumentarán la resistencia frente a los ataques de seguridad de la información. La evaluación de esta cláusula se enfocó básicamente en la gestión de no conformidades y las acciones correctivas emprendidas para su eliminación, lo que contribuye a la mejora del sistema de gestión de seguridad de la información, en este requisito el nivel de cumplimiento promedio fue de 33%.

3.3 Interacción entre Seguridad de la Información y Sistemas de información gerencial

De los resultados alcanzados y precisados anteriormente, surgen los siguientes aspectos claves para consideración:

Es importante destacar que aún existe una tendencia generalizada en las empresas estudiadas a realizar procesos de comunicación informales, tal como lo expresaron los informantes claves. Cuando se

programan reuniones formales con el personal, no existe una agenda muy precisa de los temas. Se destaca también la presencia de un proceso de información jerárquico de tipo vertical que privilegia la autoridad y que no facilita la toma de decisiones participativa que incorporen al personal en general. Se pudo notar que los SIG estudiados en la presente investigación se caracterizan por privilegiar la parte de registro de tipo financiero y contable, considerando poco los procesos medulares, documentación de éxitos o fracasos, procesos de innovación, entre otros, destacando que su implementación obedece a más bién a un enfoque cartesiano, simplificador y donde prevalecen los principios de autoridad, dirección y control que se alejan de la inspiración sistémica y en el enfoque de procesos que promueve la norma ISO 27001, en los que enfatizan investigaciones importantes en esta temática (Qi, Qingling, Wei, & Jine, 2012).

En base a la investigación de campo se verificó que las empresas participantes en el estudio mostraron diferentes niveles de tecnología en el manejo de la información. La mayoría posee algún software especializado básico que les permite realizar los registros contables y otros procesos de personal como la nómina e información relativa a algunos aspectos claves operacionales y a otros procesos internos. Es de destacar que la mayor parte de la información manejada en los sistemas de información gerencial es solo del conocimiento de los gerentes y dueños de la empresa, lo cual se convierte en un aspecto negativo y factor inhibidor para el desempeño exitoso de un SIG (Kock, Schulz, Kopmann, & Gemünden, 2020).

De la evaluación de los sistemas de información gerencial en base a los requisitos de la norma ISO 27001, se destaca que las mismas tienen un nivel de cumplimiento débil, cuyo promedio general consolidado se ubica en 39%, en lo que respecto a los mínimos elementos con los cuales debe contar un sistema de gestión de seguridad de la información, destacando los siguientes aspectos: no se encuentran desarrollados los procesos de seguridad de la información y los métodos de su implementación; se evidencia debilidad en el desarrollo y establecimiento de correspondencia de objetivos, políticas y procedimientos de seguridad de la información con los objetivos comerciales y operacionales. También se destaca que no se evidencia un enfoque formal para la implementación del sistema de gestión de seguridad de la información con la cultura corporativa; el personal de niveles jerárquicos altos no cuentan con elementos de comprensión de los requisitos de seguridad de la información; no se cuentan con indicadores medibles para evaluar la efectividad de la gestión de seguridad de la información y propuestas para su mejora. Se destaca de igual manera que las debilidades mencionadas impactan en la manera

como se gestionan los riesgos asociados a la gestión de la información, impactando negativamente la eficacia de las acciones adoptadas para evitar o mitigar los riesgos, por lo cual se evidencian fallas importantes en la adopción de una cultura de pensamiento basado en riesgo (International Organization for Standarization, 2013)

4. CONCLUSIONES

Del estudio llevado a cabo surgen las siguientes conclusiones principales:

El desarrollo de los sistemas de información gerencial (SIG) en el grupo de empresas estudiadas aun cuando tienen sus particularidades adaptados a su naturaleza, forma de operación y organización, se lograron identificar suficientes elementos comunes a partir de lo cual se caracterizó el proceso de implementación en un esquema secuencial de instauración del SIG conformado por ocho etapas o fases que inician con la planificación del SIG y concluye con la documentación de éste.

La evaluación de los sistemas de información gerencial implementados en función de los requisitos previstos en la norma ISO 27001: 2013, relacionado con la seguridad de la información, deja en evidencia que las empresas de servicios de ensayos no destructivos en Lima – Perú, muestran un nivel incipiente en lo que respecta a la integración de aspectos de seguridad de la información en sus respectivos SIG, presentando mayor debilidad en los requisitos relacionados con la evaluación del desempeño y mejora.

Las empresas participantes en la investigación evidenciaron el interés de hacer de la información fuente de ventaja competitiva para las mismas, aun cuando los sistemas actuales muestran especial énfasis a la gestión de información de tipo financiera y contable. Existe el interés general de evolucionar a gestionar la información asociada a los procesos operacionales de la misma manera como se gestiona la información contable.

5. REFERENCIAS BIBLIOGRÁFICAS

Andreau, R., Ricart, J., & Valor, J. (2016). *Estrategias y sistemas de información.* Méxíco: Mc Graw Hill.

Arteaga, F., Cardenas, G., & D. R. (2016). *Fundamentos de sistemas de información gerencial.* España: EAE.

Bagad, V. (2015). *Management Information Systema.* Universidad Pedagógica Nacional. India: Tecnical

Publications Pune.

Davis, G., & Olson, M. (2016). *Sistemas de Información Gerencial.* México: Mc Graw Hill.

Drucker, P. (2015). *Las nuevas realidades.* Barcelona . España: EDHASSA.

Gauchi, V. (2012). Aproximación teórica a la relación entre los términos gestión documental, gestión de la información y gestión del conocimiento. *Revista española de documentación ceintífica*, 531-554.

Heeks, R. (2007). *Information technology and public sector corruption: Institute for Development Policy and Management,*. University of Manchester, Manchester.

Hernández Sampieri, R. (2014). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta.* México: McGraw Hill.

Hernández, A. (2011). Los sistemas de información: Evolución y Desarrollo. *Revista de relaciones laborales*, 149-165.

International Organization for Standarization. (2013). *Sistema de Gestión de Seguridad de la Información.* Ginebra: ISO.

Kock, A., Schulz, B., Kopmann, J., & Gemünden, H. (2020). Project portfolio management information systems' positive influence on performance – the importance of process maturity. *International journal of project management*, 229-241.

Larrocha, E. (2017). *Nuevas tendencias en los sistemas de información.* Madrid: Editorial Universitaria Ramón Areces.

Laudon, K. (2016). *Sistemas de Información Gerencial* (14 ed.). México: Pearson.

Nonaka, I., & Byosiere, P. (2010). *La creación de conocimiento regional un proceso de desarrollo social.* Bilbao - España.

Porter, M. (2015). *Estratégia Competitiva. Técnicas para el análisis de los sectores industriales y de la competencia.* México: Grupo Editorial Patria.

Qi, L., Qingling, D., Wei, S., & Jine, Z. (2012). Modeling of Risk Treatment Measurement Model under Four Clusters Standards (ISO 9001, 14001, 27001, OHSAS 18001). *Procedia Engineering. Volume 37*, 354-358.

Saez López, J. (2017). *Investigación educativa. Fundamentos teóricos, procesos y elemntos prácticos.* México: UNED.

Syreyshchikova, N., Pimenov, D., Mikolajczyk, T., & Moldovan, L. (2019). Information Safety Process Development According to ISO 27001 for an industrial enterprise. *Procedia Manufacturin*, 278-285.