UNIVERSIDAD PERUANA UNIÓN

FACULTAD DE INGENIERÍA Y ARQUITECTURA

Escuela Profesional de Ingeniería de Sistemas

Criterios y aspectos evaluados por las empresas al implantar un sistema de gestión de seguridad de la información

Por:

Isaí Natán Caruajulca Bravo

Asesor:

Dr. Miguel Angel Valles Coral

Tarapoto, setiembre de 2020

DECLARACIÓN JURADA
DE AUTORIA DE TRABAJO DE INVESTIGACIÓN

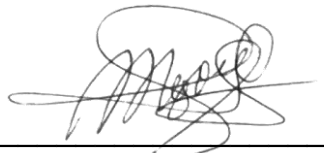
Yo, Miguel Angel Valles Coral, de la Facultad de Ingeniería de Sistemas, Escuela Profesional de Ingeniería de Sistemas, de la Universidad Peruana Unión.

DECLARO:

Que el presente informe de investigación titulado: “CRITERIOS Y ASPECTOS EVALUADOS POR LAS EMPRESAS AL IMPLANTAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN” constituye la memoria que presenta el Bachiller Caruajulca Bravo, Isaí Natán; para aspirar al Grado Académico de Bachiller en Ingeniería de Sistemas cuyo trabajo de investigación ha sido realizado en la Universidad Peruana Unión bajo mi dirección.

Las opiniones y declaraciones en este informe son de entera responsabilidad del autor, sin comprometer a la institución.

Y estando de acuerdo, firmo la presente constancia en Morales, a los 03 días del mes de setiembre del año 2020.



Asesor
Dr. Miguel Angel Valles Coral

Criterios y aspectos evaluados por las empresas al implantar un sistema de gestión de seguridad de la información

TRABAJO DE INVESTIGACIÓN

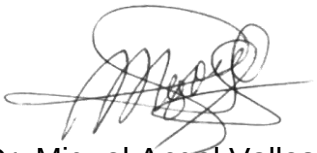
Presentado para optar el Grado de Bachiller en Ingeniería de Sistemas

JURADO CALIFICADOR

Mg. Immer Elías Cuellar Rodriguez
Presidente

Mg. Joseph Ibrahim Cruz Rodriguez
Secretario

Mg. Danny Lévano Rodriguez
Vocal



Dr. Miguel Angel Valles Coral
Asesor

Tarapoto, setiembre de 2020

Resumen

Esta investigación tiene como objetivo realizar un análisis de los criterios y aspectos al implementar un sistema de gestión de seguridad de la información (SGSI) sobre las empresas, permitiendo identificar mejores procedimientos para ser aplicados ante situaciones perjudiciales. Las tecnologías de información y comunicaciones(TIC) han colocado un gran interés a la protección de la información para garantizar apropiados niveles de seguridad y preservación. Para el desarrollo de la revisión se hizo un bosquejo sobre artículos a nivel internacional referente al proceso que se llevó al implementar una adecuada gestión de seguridad, basadas en algunas buenas practicas, metodologías y estándares. Se concluye que, al implementar una buena gestión, permite mejorar la situación actual que viven las empresas en materia de seguridad de la información y a la vez, estos criterios y aspectos de éxito sirvan como una guía y modelo a aquellos que están implementando un SGSI para alguna empresa.

Palabras claves: criterios; aspectos; gestión de seguridad de la información; buenas practicas; estándares.

Abstract

This research aims to carry out an analysis of the criteria and aspects when implementing an information security management system (ISMS) about companies, which allows identifying better procedures to apply in harmful situations. Information and communication technologies (ICT) have placed great interest in the protection of information to guarantee appropriate levels of security and preservation. For the development of the review, an outline was made on articles at the international level regarding the process that was carried out when implementing adequate security management, based on some good practices, methodologies and standards. It is concluded that, by implementing good management, it allows to improve the current situation that companies live in the area of information security and at the same time, these criteria and aspects of success serve as a guide and model for those who are implementing an ISMS to some company.

Keywords: criteria; aspects; Information security management; good practices; standards

1. Introducción

A 2020, las empresas y organizaciones de todo el mundo utilizan las ventajas competitivas de las Tecnologías de la Información y Comunicaciones (Cano-Pita, 2018) y han colocado un gran interés a la protección de su información para así afrontar vulnerabilidades presentes que continuamente se convierten en amenazas (Tejena-Macía, 2018), siendo la información un activo primordial en el ámbito empresarial, es necesario garantizar apropiados niveles de seguridad e implica tener una adecuada utilización y preservación de la información, ya que es el más importante a rescatar y salvaguardar (Altamirano, 2019).

Cabe resaltar que muchas son las entidades que carecen de un análisis de valoración y gestión de su información lo cual da lugar a la manipulación, divulgación, o simplemente la falta de disponibilidad causada por incidentes en la seguridad (Gil y Gil, 2017) que pueden ocasionar robo de información, sustracción de data sensible de clientes, pérdida de credibilidad y hasta daños financieros, lo que afectaría directamente la sostenibilidad de las entidades (Tejena-Macía, 2018).

A su vez, se reconoce que las personas juegan un papel crucial en la seguridad de la información, que es el elemento vital de una empresa. Sin embargo, se determinó que la mayoría de estos incidentes de seguridad reportados y las infracciones dentro de las organizaciones se deben a errores humanos (Evans, He, Maglaras, Yevseyeva y Janicke, 2019), que resultan en incidentes e infracciones regulares y un amplio nivel de exposición al riesgo que no puede ignorarse dentro de la seguridad de la información (Evans, He, Luo, et al., 2019).

Los problemas de la seguridad de la información se relacionan con el desconocimiento sobre la aplicación de las normas y las limitaciones con la administración adecuada a la seguridad (Stuart, Rodríguez, Martínez, Cordero y Delgado, 2017); algunos criterios importantes por la cual se deriva esta problemática, es la falta de organización del SGSI, documentación incompleta u obsoleta del SGSI, falta de análisis de riesgos regulares, falta de revisiones, auditorías o controles, uso limitado de medidas de protección

física y tecnológica, falta de capacitación o desarrollo profesional (Szczepaniuk, Szczepaniuk, Rokicki y Klepacki, 2020).

Por lo anterior la presente revisión ha realizado un análisis de los criterios y aspectos de las empresas al implementar un sistema de gestión de seguridad de la información, la cual ha permitido identificar mejores procedimientos que se llevan a cabo en distintas situaciones, ya que la utilización de estándares internacionales y buenas prácticas, repercuten directamente en una efectiva gestión de la información; en fin, se pretende que estos criterios de éxito sirva como una guía o modelo a aquellos ingenieros que están en la etapa de implementar un SGSI para alguna empresa.

2. Metodología

Para el desarrollo de este artículo, en primer lugar, se analizó los distintos criterios de seguridad de la información aplicadas a distintas empresas con propósitos muy específicos para tomar en consideración el proceso de aplicabilidad que se conlleva durante la implementación de un sistema de gestión de seguridad de la información, comprendió revisiones secundarias y publicaciones de revistas.

En la actualidad existen diversos tipos de clasificación, el que se aplicó en este trabajo es una revisión integradora, porque se revisaron artículos desarrollados en distintos países referente al proceso que se llevó al implementar una adecuada gestión de seguridad basadas en algunas o buenas practicas, metodología y estándares o normas durante la aplicabilidad.

En segundo lugar, para la obtención de los artículos de referencia se tuvo en cuenta algunos motores de búsqueda, particularmente académicas y científicas tales como: Google Scholar, EBSCO y ScienceDirect, teniendo en cuenta que cada artículo tomado esté indexado en Latindex como mínimo y en preferencia IEEE, Scopus, WoS y Scielo; como parte fundamental se tuvo en cuenta el límite de años a los que debían comprender cada artículo adquirido, por la que optamos entre 2016 a 2020 respectivamente.

Como último paso, para la organización y estructura de los datos se realizó un bosquejo referente a la gestión de seguridad del a información, de esta forma se presenta una visión general del estado actual del trabajo de revisión, teniendo en cuenta nuestro alcance, de tal modo que siga un orden lógico y sistemático.

3. Desarrollo

3.1. La información

La información es un bien fundamental para el funcionamiento y ejecución estratégica de las empresas, siendo el activo más importante de una organización se debe establecer medidas de protección para reducir el riesgo de ataques (Martelo, Tovar y Maza, 2018).

El factor clave de la información, es su valor como fuente de conocimientos imprescindibles para a la conducción y comprensión de situaciones, como la capacidad para fundamentar, investigar, elaborar planes políticas, económicas y financieras y así resolver los conflictos y lograr una correcta toma de decisiones (Rodríguez, Mho y Ramírez, 2017).

Siendo la información un activo valioso, a menudo esta es almacenada en equipos o soportes de información o son transferidos de un lugar a otro por medios de transmisión de datos, por ello se hace necesario brindarles una protección adecuada debido a se producen violaciones a la seguridad de información derivadas de las vulnerabilidades existentes en los sistemas de seguridad (Yupanqui y Bayona, 2017).

3.2. Sistema de gestión de seguridad de la información

La Organización Internacional para la Estandarización (ISO), define a los SGSI como un enfoque sistemático para reforzar las restricciones contra los comportamientos de seguridad indeseable y administrar la información sensible de la compañía como para que permanezca segura. Esto ayuda a que las empresas mantengan seguros los activos de información (Yupanqui y Bayona, 2017).

La gestión de seguridad de la información debe estar orientada a proteger la propiedad intelectual y los activos de información basado en estándares y metodologías que permiten minimizar los riesgos y optimizar las inversiones de las organizaciones, implementando estas acciones permitirá identificar el grado de exposición y las amenazas que puedan afectar la organización (Figueroa-Suárez, Rodríguez-Andrade, Bone-Obando y

Saltos-Gómez, 2017). Una amenaza puede afectar la posibilidad de que las organizaciones puedan desarrollar sus actividades, dando problemas a la información o los sistemas que la procesan.

Las áreas de las TIC tienen como propósito mantener los niveles aceptables de riesgo de la información y toman a la gestión de seguridad de la información como una disciplina, que al ser gestionada se debe tener como base primordial una política de seguridad, para tener en cuenta los procesos reglamentarios aplicables, requisitos legales y el compromiso de la alta gerencia para conseguirlos (Valencia-Duque y Orozco-Alzate, 2017).

3.3. Proceso de implementación de los sistemas de gestión de seguridad de la información

El implementar un sistema de gestión de seguridad de la información es vital para la supervivencia de la empresa del siglo XXI, por tanto, debe ser considerado en todo plan estratégico organizacional. Cedeño define al SGSI como modelo estratégico diseñado para toda organización donde se requiere establecer, implementar, operar, supervisar y mejorar la seguridad de la información, la que permitirá a toda organización que cumpla con sus lineamientos para obtener una certificación internacional (Cedeño, 2018).

Según Miranda, el proceso para establecer y manejar un SGSI implica relacionar las siguientes actividades: Establecer: Define los objetivos de control y el alcance del SGSI, a partir del análisis de riesgos realizado y especificar los procedimientos de operación. Implementar: Implementar los controles y definir cómo medir la efectividad. Operar: Llevar las acciones necesarias para la ejecución de los procedimientos. Monitorizar: Supervisar el funcionamiento de los controles con el objetivo de detectar errores e identificar incidentes y violaciones. Revisar: Evaluar la efectividad del SGSI, respecto al cumplimiento de los objetivos. Mantener y mejorar: Realizar acciones correctivas e implementar las mejoras (Miranda, Valdés, Pérez, Portelles, y Sánchez, 2016).

El uso de protocolos de seguridad y métodos de encriptación durante la implementación de un SGSI, permite el cifrado y descifrado de la información, esto conlleva a que la seguridad pueda garantizar la confidencialidad y autenticidad; se afirma que estos métodos producen excelentes resultados durante el uso de recursos computacionales (Solís, Pinto, y Solís, 2017).

3.4. Criterios y aspectos evaluados por las empresas al implantar un sistema de gestión de seguridad de la información

En Polonia, el Marco Nacional de Interoperabilidad obligó a las entidades del sector de finanzas públicas a implementar un sistema de gestión de seguridad de la información resguardando los aspectos como la deficiente organización de un SGSI, carente evaluación de riesgos, bajo nivel de auditorías o controles, uso limitado de medidas de seguridad físicas y técnicas y la baja capacitación o desarrollo profesional. La implementación de las soluciones de la Unión Europea bajo los principios del Reglamento General de Protección de Datos (Reglamento GDPR), la orden de la Ley de Protección de Datos Personales y la Ley de Ciberseguridad Nacional, resultó en un aumento sobre el nivel de seguridad de la información, ciberseguridad de redes y la protección de la privacidad general, permitiendo reducir significativamente la aparición de irregularidades identificadas (Szczepaniuk et al., 2020).

Se han desarrollado investigaciones en Cuba, donde se muestra que las empresas toman continuidad sobre la seguridad de la información para elevar la eficiencia de los sistemas; este país al implementar una norma de seguridad internacional, lo constituyen como una buena práctica, ya que es necesaria para garantizar la competitividad entre las organizaciones y la seguridad de la información de los clientes. Entonces el criterio más importante a tomar en cuenta de las empresas cubanas han sido las capacitaciones dirigidas al personal, en la cual se desarrollaron cursos intensivos sobre el manejo de los sistemas de información, además otro punto fue la aplicación de acciones, en la cual

establecen los pasos necesarios para la implementación de un SGSI y todo ello hasta llegar a la certificación de la empresa (Castillo y Pérez, 2017).

A su vez, el gobierno de Colombia ha impulsado a las empresas a implementar tecnologías, estándares y marcos de referencias de seguridad relacionadas al control de la información, gestión de servicios y gobierno de TI, con el fin de prevalecer en la globalización respecto al uso adecuado de las tecnologías, manteniéndolas seguras y utilizándolas para prestar servicios adecuados. Un aspecto importante de las empresas colombianas es que los trabajadores utilizan buenas prácticas respecto a la seguridad de la información, pero de manera “divergente” o “independiente” tratando de cumplir los requisitos legales, la cual es un punto de conocimiento necesario para la aplicación de un SGSI (Castro, Velásquez y Castro, 2018).

En Noruega se ha desarrollado un SGSI con entorno a Big Data para recopilar y procesar grandes cantidades de información de una amplia gama de campos; toma a la seguridad de la información como una gobernanza y que este es el pegamento que genera valor y mitiga el riesgo. Un 58% de las organizaciones que informaron haber realizado esfuerzos activos de big data, han propuesto distintos aspectos para una adecuada gobernanza de la seguridad de la información, una de ellas ha sido crear entornos restringidos para el análisis seguro de datos, seguido de realizar respaldados por una protección y gobernanza robusta, y como último punto se ha propuesto desarrollar un proceso de mitigación de riesgos y de medición de seguridad, para controlar el riesgo de un activo dispuesto por TI; esto ha ayudado aumentar el valor del capital intelectual de las organizaciones de "economía de la información", su viabilidad comercial y rentabilidad financiera (Moghadam y Colomo-Palacios, 2018).

Los casos de Perú han reflejado una realidad no muy distinta a los demás países, dado que la evaluación de los sistemas de información gerencial se ha basado en los requisitos de la normas y estándares relacionados a la seguridad de la información, a diferencia de que se posee un nivel de cumplimiento débil, cuyo promedio general consolidado se ubica en 39% debido a que los aspectos que debe contar un SGSI no se

encuentran desarrollados, como: los procesos de seguridad de la información y los métodos de su implementación (Lugo, Carrasquero y Gómez, 2020). Uno de los criterios fundamentales de Polonia y Cuba han sido las capacitaciones dirigidas a su personal, la cual es muy esencial aplicarlo a todas nuestras entidades peruanas, ya que es necesario tener trabajadores capaces de manejar los procesos de seguridad de la información. Por otro lado, Colombia ínsita un aspecto importante en la que cada trabajador aplica seguridad a la información de manera “divergente” o “independiente” la cual es muy esencial, esta debe servir como modelo de una iniciativa para la implementación de un SGSI dentro de nuestras empresas peruanas.

4. Conclusiones

En general, la evolución del sistema de gestión de seguridad de la información se ha dado como resultado de los cambios en la normatividad legal (Riaño-Casallas, Hoyos y Valero, 2016), por ello, implementar una buena gestión de seguridad de la información ha permitido mejorar la situación de las empresas afinando así las capacidades de detección y contención de posibles amenazas en el entorno del negocio, ya que la utilización de estándares internacionales y buenas prácticas, repercuten directamente en una efectiva gestión de seguridad, garantizando el cumplimiento de los principios (Cano y Almanza, 2019).

La naturaleza de las amenazas a la seguridad de la información es más sofisticada y sin precedentes en términos de prevención, mitigación de riesgos y seguridad de la información, podrían dar lugar a graves pérdidas económicas. Se han analizado los criterios y aspectos relacionados en el marco de trabajo integral de la SGSI en las organizaciones y se ha definido que es necesario integrar la seguridad de la información en la gestión empresarial a través del desarrollo de un marco de gobernanza (Cárdenas-Solano, Martínez-Ardila y Becerra-Ardila, 2016).

En el trabajo desarrollado, se ha evidenciado como las empresas trataron de prevenir las situaciones, en las cuales se pudo haber presentado un siniestro que signifique una paralización de las operaciones o consecuentes a ellas, se han mostrado algunos puntos claves para una adecuada implementación y gracias a ello se ha reflejado una disminución de la complejidad y un aumento de eficiente seguridad de la información tras la implementación de controles automatizados basados en una SGSI (Miranda et al., 2016).

Por lo anterior la presente revisión concluye mostrando los criterios y aspectos evaluados por las empresas al implementar un sistema de gestión de seguridad de la información, la cual ha permitido realizar un análisis para identificar mejores procedimientos que pueden darse en la gestión de la información, ya que teniendo en cuenta los criterios y aspectos al implementar un estándar internacional y buenas prácticas, repercutirán directamente en una efectiva gestión de la información y sus procesos; por otra parte,

queremos que estos criterios de éxito, sirva como una guía o modelo a aquellos ingenieros que están en la etapa de implementar un SGSI para alguna empresa.

5. Referencias

Altamirano, M. (2019). Modelo para la gestión de la seguridad de la información y los riesgos asociados a su uso. Avances (Centro de Información y Gestión Tecnológica), 21(2), 248–263. Recuperado de http://www.ciget.pinar.cu/ojs/index.php/publicaciones/article/view/440

Cano-Pita, G. E. (2018). Las TICs en las empresas: evolución de la tecnología y cambio estructural en las organizaciones. Dominio de las Ciencias, 4(1), 499–510. https://doi.org/10.23857/dc.v4i1.762

Cano, J., y Almanza, A. (2019). Estudio de la evolución de la Seguridad de la Información en Colombia : 2000 - 2018. Revista Iberica de Sistemas y Tecnologias de Información, 470–484. Recuperado de https://search.proquest.com/docview/2385758173?pq-origsite=gscholar&fromopenview=true

Cárdenas-Solano, L.-J., Martínez-Ardila, H., y Becerra-Ardila, L.-E. (2016). Gestión de seguridad de la información: revisión bibliográfica. El Profesional de la Información, 25(6), 931–948. https://doi.org/10.3145/epi.2016.nov.10

Castillo, G., y Pérez, E. (2017). Diagnóstico de los sistemas de información en las empresas priorizadas según los requerimientos actuales. Centro de información y gestión tecnológica, 6(2), 22. https://doi.org/10.24215/PCe022

Castro, D., Velásquez, T., y Castro, H. (2018). Integración de seguridad y gestión de servicios en el gobierno de las tecnologías de la información. Revista Colombiana de Tecnologías de Avanzada, 2(32), 62–67. https://doi.org/10.24054/16927257.v32.n32.2018.3027

Cedeño, R. (2018). La seguridad de la información: Aspecto crucial que toda empresa del siglo XXI debe gestionar. Revista Científica Ciencia y Tecnología, 18(18), 210–220. Recuperado de http://cienciaytecnologia.uteg.edu.ec/revista/index.php/cienciaytecnologia/article/view/453/460

Evans, M., He, Y., Luo, C., Yevseyeva, I., Janicke, H., y Maglaras, L. A. (2019). Employee perspective on information security related human error in healthcare: Proactive use of IS-CHEC in questionnaire form. IEEE Access, 7, 102087–102101. https://doi.org/10.1109/access.2019.2927195

Evans, M., He, Y., Maglaras, L., Yevseyeva, I., y Janicke, H. (2019). Evaluating information security core human error causes (IS-CHEC) technique in public sector and comparison with the private sector. International Journal of Medical Informatics, 127, 109–119. https://doi.org/10.1016/j.ijmedinf.2019.04.019

Figueroa-Suárez, J. A., Rodríguez-Andrade, R. F., Bone-Obando, C. C., y Saltos-Gómez, J. A. (2017). La seguridad informática y la seguridad de la información. Polo del Conocimiento, 2(12), 145–155. https://doi.org/10.23857/pc.v2i12.420

Gil, V. D., y Gil, J. C. (2017). Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas Informatic organizational security: a simulation model based on systems dynamic. Scientia et Technica, 22(2), 193–197. https://doi.org/10.22517/23447214.11371%0A

Lugo, J., Carrasquero, H., y Gómez, J. (2020). Evaluación de gestión de seguridad de la información en los sistemas de información general como herramienta de competitividad en empresas de servicios de ensayos no destructivos en la ciudad de Lima - Perú. Revista Científica QUALITAS, 19, 62–76. Recuperado de https://revistas.unibe.edu.ec/index.php/qualitas/article/view/42

Martelo, R. J., Tovar, L. C., y Maza, D. A. (2018). Modelo básico de seguridad lógica. Caso de estudio: el laboratorio de redes de la Universidad de Cartagena en Colombia. Informacion Tecnologica, 29(1), 3–10. https://doi.org/10.4067/S0718-07642018000100003

Miranda, M., Valdés, O., Pérez, I., Portelles, R., y Sánchez, R. (2016). Metodología para la implementación de la gestión automatizada de controles de seguridad informática. Revista Cubana de Ciencias Informáticas, 10(10), 14–26. Recuperado de https://rcci.uci.cu/?journal=rcci&page=article&op=view&path%5B%5D=987

Moghadam, R. S., y Colomo-Palacios, R. (2018). Information security governance in big data environments: A systematic mapping. Procedia Computer Science, 138, 401–408. https://doi.org/10.1016/j.procs.2018.10.057

Riaño-Casallas, M. I., Hoyos, E., y Valero, I. (2016). Evolución de un sistema de gestión de seguridad y salud en el trabajo e impacto en la accidentalidad laboral: Estudio de caso en empresas del sector petroquímico en Colombia. Ciencia & trabajo, 18(55), 68–72. https://doi.org/10.4067/s0718-24492016000100011

Rodríguez, M., Mho, J., y Ramírez, R. (2017). Infotecnología y gestión de la información en la carrera de economía. Transformación, 13(1), 139–149. Recuperado de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2077-29552017000100014

Solís, F., Pinto, D., y Solís, S. (2017). Seguridad de la información en el intercambio de datos entre dispositivos móviles con sistema android utilizando el método de encriptación RSA. Enfoque UTE, 8(1), 160–171. https://doi.org/10.29019/enfoqueute.v8n1.123

Stuart, M., Rodríguez, D., Martínez, Y., Cordero, A., y Delgado, T. (2017). Experiencia en el diagnóstico de la gestión de información con enfoque de arquitectura de información empresarial. Revista Internacional de Gestión del Conocimiento y la Tecnología, 5(1), 1–16. Recuperado de https://www.upo.es/revistas/index.php/gecontec/article/view/1897

Szczepaniuk, E. K., Szczepaniuk, H., Rokicki, T., y Klepacki, B. (2020). Information security assessment in public administration. Computers and Security, 90. https://doi.org/10.1016/j.cose.2019.101709

Tejena-Macía, M. A. (2018). Análisis de riesgos en seguridad de la información. Polo del Conocimiento, 3(4), 230–244. https://doi.org/10.23857/pc.v3i4.809

Valencia-Duque, F. J., y Orozco-Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. RISTI - Revista Ibérica de Sistemas y Tecnologias de Información, (22), 73–88. https://doi.org/10.17013/risti.22.73-88

Yupanqui, J., y Bayona, S. (2017). Políticas de seguridad de la información: Revisión sistemática de las teorías que explican su cumplimiento. Revista Iberica de Sistemas e Tecnologias de Informacao, 2017(25), 112–134. https://doi.org/10.17013/risti.25.112-134