INNOVA Research Journal 2018, Vol 3, No. 2.1, 93-99
ISSN 2477-9024

Diseño de un Plan Estratégico de Seguridad de la Información, Mediante la Aplicación de Análisis de Riesgos con la Norma ISO/IEC 27005 Caso de Estudio INAMHI

Design of a Strategic Plan for Information Security, through the Application of Risk Analysis with ISO / IEC 27005 Case Study INAMHI

Diego Gonzales
Universidad Internacional SEK
Autor para correspondencia:diegofabian2005@hotmail.com
Fecha de recepción: 15 de diciembre 2017 - Fecha de aceptación: 26 de febrero de 2018

Resumen: En la investigación se realizó a las instituciones del Estado Ecuatoriano, encontrando la necesidad de una gestión adecuada de la información permitiendo la evaluación de la infraestructura, los sistemas de información y las medidas organizacionales desde la perspectiva tecnológica. En este estudio se utilizó el método inductivo-deductivo que con un enfoque experimental permitió la solución al problema del manejo desordenado de la información. En el estudio se realizó una auditoria por parte del ente rector al EGSI y permitió establecer un punto de partida, para luego con el análisis del riesgo y la norma ISO/IEC 27005:2012 - OCTAVE-S obtener los controles, políticas y procedimientos de seguridad de la información, las mismas que se pondrán en ejecución por parte del comité de seguridad de la información de la institución estudiada, permitiendo una mejor gestión del riesgo.
Palabras clave: Gestión de riesgos, ISO 27005, Seguridad de la Información, OCTAVE-S

Abstract: The research was carried out to the Ecuadorian State institutions, finding the need for an adequate management of the information allowing the evaluation of the infrastructure, the information systems and the organizational measures from the technological perspective. In this study, we used the inductive-deductive method that with an experimental approach allowed the solution to the problem of the disorderly handling of information. In the study an audit was conducted by the governing body to the EGSI and allowed to establish a starting point, then with the risk analysis and ISO / IEC 27005: 2012 - OCTAVE- S obtain the controls, policies and procedures of security of information, which will be implemented by the information security committee of the institution studied, allowing better risk management.
Keywords: Risk Management, ISO 27005, Information Security, OCTAVE-S

Introducción

Hoy en día, la informática se ha convertido en un factor importante en el cumplimiento de los objetivos institucionales, los sistemas de información están basados en necesidades que son gestionadas mediante la automatización de procesos que ayudan a la alta gerencia en la toma de decisiones, estas se caracterizan por dotar de ventajas en dimensiones cómo la oportunidad, confiabilidad y efectividad, respecto a la planificación, facilitan los procesos de programación y administración, con el fin de garantizar su éxito, minimizar el riesgo y reducir costos asociados a la gestión.

La información que se maneja tanto al interior de una institución como hacia al exterior de la misma, está expuesta a un gran número de riesgos, los cuales tienen un impacto considerable, que puede afectar la confidencialidad, integridad y disponibilidad de la información. También, el principal reto está en gestionar adecuadamente los riesgos específicos para cada entorno del negocio en particular y también entender mediante una adecuada medición, el impacto que estos riesgos tienen sobre la organización.

Debido a esta razón, nace en las entidades públicas la necesidad de implementar nuevos sistemas de seguridad de la información, con el objeto de fortalecer las políticas y procedimientos de uso, estando supeditadas incluso a políticas a nivel de entes de control, encargadas de verificar que se administren y gestionen eficientemente.

Se requiere entonces considerar, la normativa existente y que rige a las instituciones públicas en el estado ecuatoriano, acuerdo ministerial 166 Esquema Gubernamental de Seguridad de la Información EGSI, la misma que en el artículo 7 manifiesta que "*Las entidades realizarán una evaluación de riesgos y diseñarán e implementarán el plan de manejo de riesgos de su institución, en base a la norma INEN ISO/IEC 27005* "Gestión del Riesgo en la Seguridad de la Información. Porque es necesario cumplir con lo dispuesto por el organismo de control.

La aplicación de un plan estratégico, correctamente diseñado, permitió asegurar la información en el Instituto Nacional de Meteorología e Hidrología, el mismo que se conformó por procesos, donde se evaluó y analizó los riesgos apoyados en políticas y estándares que satisficieron las necesidades del INAMHI en materia de seguridad.

La consecución del objetivo de la investigación se basó en el análisis de riesgos con la norma ISO 27005:2011, misma que contiene las recomendaciones y directrices generales para la gestión de riesgo y de esta manera facilitó la determinación de los controles y procedimientos que permitieron mejorar significativamente la gestión del riesgo.

El proceso de gestión del riesgo de la seguridad de la información puede ser iterativo para las actividades de valoración y tratamiento del riesgo. Un enfoque iterativo para realizar la valoración del riesgo permite incrementar la profundidad y el detalle de la valoración en cada iteración. El enfoque iterativo suministra un buen equilibrio entre la reducción del tiempo y el esfuerzo requerido para identificar los controles, incluso garantizando que los riesgos altos se valoren de manera correcta. (ISO 27005:2012)

Una vez que se ha podido establecer el contexto, se realiza una valoración del riesgo, si ésta suministra información suficiente para determinar de manera eficaz las acciones que se necesitan para modificar los nivelas de riesgo hasta un nivel aceptable, entonces la labor está terminada y se puede establecer un mecanismo para el subsiguiente tratamiento del riesgo.

Si la información no es suficiente, se llevará a cabo otra iteración de la valoración del riesgo con un contexto revisado, por ejemplo, los criterios de evaluación del riesgo, los criterios de aceptación el riesgo o los criterios de impacto, posiblemente en partes específicas del alcance total. (ISO 27005:2012)

Es importante diseñar un plan de seguridad de la información basado en el análisis de riesgos porque permite establecer los controles con el propósito de gestionar los riesgos, además de cumplir con la normativa emitida por el organismo de control y las evaluaciones anuales al EGSI de las instituciones públicas del estado ecuatoriano.

Método

Se utilizó la metodología OCTAVE-S, misma que se fusionó con la norma ISO 27005:2011, permitiendo que las personas de la organización asuman la responsabilidad de establecer la estrategia de seguridad de la organización. La técnica aprovechó los conocimientos de las prácticas y los procesos relacionados con la seguridad de la organización para capturar el estado actual de la seguridad dentro de la misma. Los riesgos para los activos más críticos se utilizaron para priorizar áreas de mejora y establecer la estrategia de seguridad de la organización. A diferencia de las evaluaciones centradas en la tecnología típica, las cuales están dirigidas a la gestión del riesgo tecnológico y se centran en cuestiones tácticas, OCTAVE está dirigido a riesgo de la organización y se centra en temas estratégicos, relacionados con la práctica. (Espinosa, Martínez, Amador, & Amador, 2014)

El enfoque OCTAVE es impulsada por dos de los aspectos: el riesgo operativo y las prácticas de seguridad. La tecnología sólo se examina en relación con las prácticas de seguridad, lo que permite a una organización afinar la vista de sus prácticas de seguridad actuales. Al utilizar el enfoque OCTAVE, una organización toma decisiones de protección de la información basada en los riesgos para la confidencialidad, integridad y disponibilidad de los activos relacionados con la información crítica. Todos los aspectos de riesgo (activos, amenazas, vulnerabilidades y el impacto sobre la organización) se tienen en cuenta en la toma de decisiones, lo que le permite a una organización que coincida con una estrategia de protección basada en la práctica de sus riesgos de seguridad. (Espinosa, Martínez, Amador, & Amador, 2014)

Resultados

Encuesta

Se realizó una encuesta al personal del INAMHI por parte del Comité de Seguridad de la Información y Gobierno Electrónico sobre el conocimiento de controles, políticas y procedimientos sobre Seguridad de la Información.

La población seleccionada es de todo el personal del INAMHI 170 funcionarios.

Tabla1: *Personal que conforman la muestra*

POBLACIÓN	PERSONAS
ADMINISTRATIVOS	40
PERSONAL TECNICO	70
PERSONAL REGIONALES	60
TOTAL	**170**

Fuente: Investigador, Elaboración propia

Análisis

Se practicó también una evaluación de los conocimientos de los funcionarios de las áreas de TI de todo el país de la institución, una vez analizados los resultados, se puede evidenciar la falta de conocimientos sobre "Seguridad de la Información" por lo que tras el análisis documental y el estudio del estado del arte se ha evaluado la aplicación de la norma ISO 27005 para la implementación de políticas de seguridad y lineamientos que se deben seguir para responder al problema de investigación.

Para la investigación se utilizó la norma ISO 27005:2012 adaptando la metodología OCTAVE-S, siguiendo el proceso detallado a continuación, para su evaluación. El contexto se estableció mediante un análisis y levantamiento de información apoyado en métodos e instrumentos de investigación debidamente validados, esto permitió realizar una valoración del riesgo. En algunos casos, ésta valoración suministró información suficiente para determinar de manera eficaz las acciones que se necesitan para gestionar oportunamente los riesgos, hasta llegar a un nivel aceptable, entonces en estos factores analizados se procedió a la documentación de dichos hitos para asegurar el tratamiento de los mismos. En aquellos casos en los que información no fue suficiente, se llevó a cabo otra iteración de la valoración del riesgo con un contexto revisado y en procura de practicar un análisis más específico que permita satisfacer los factores que no se pudieron abarcar en la anterior revisión. (ISO:27005:2012, 2017)

Se realizó el análisis de riesgos a la parte de telecomunicaciones y hardware del departamento de tecnologías de la información y comunicación del INAMHI:

Análisis de riesgos

Sistema de telecomunicaciones

1. Sistema telefonía IP es deficiente y por lo tanto no funciona de manera adecuada
2. Perdida de información constantes por intermitencias en sistemas de comunicación como correo institucional o más servicios dependientes de estas tecnologías.

Hardware

3. Falta de mantenimiento correctivo a equipos Hardware
4. Instalación de equipos de cómputo en la institución
5. Falta de procedimientos que indique como restaurar la interconexión entre sedes

Se realizó el tratamiento, las observaciones respectivas para luego obtener los controles que permitirán gestionar el riesgo.

Controles

Tipo de control: preventivo 1.

ISO 27001: 10.3

Planificación y Aceptación del Sistema.

En su defecto posible montaje de sistema VoIP propio.

Tipo de control: preventivo /correctivo 2.

ISO 27001: 10.3

Planificación y Aceptación del Sistema.

En su defecto posible contratar a una empresa externa para su administración.

Tipo de control: preventivo /correctivo 3.

ISO 27001: 9.2.4

Mantenimiento de equipos.

Tipo de control: preventivo /correctivo 4.

ISO 27001: 9.2.4

Mantenimiento de equipos.

Tipo de control: preventivo /correctivo

5. ISO 27001: 10.1.1 Procedimientos operativos documenta dos

ISO 27001: 14.1.3 Mantener o restaurar operaciones para asegurar la disponibilidad de la información.

Discusión

En el sector público ecuatoriano, se dificulta cumplir con las leyes y normativas dispuestas por los organismos de control, el acuerdo ministerial 166 EGSI manifiesta que las entidades deben realizar evaluaciones de riesgos y diseñarán e implementarán el plan de manejo de riesgos de su institución, en base a la norma INEN ISO/IEC 27005 Gestión del Riesgo en la Seguridad de la Información. Por lo que la investigación propuesta, dotará de herramientas a otras instituciones para cumplir con lo dispuesto por el organismo de control.

En la actualidad los organismos de control establecieron un cronograma anual para proceder a las revisiones del EGSI, de esta manera sancionar a las instituciones que no disponen de un plan de seguridad de la información que es muy diferente a un plan estratégico de Tecnologías de la información, tal y como se explica en este caso de estudio que siguiendo la metodología planteada como ISO 27005:2012 con OCTAVE-S se logra establecer controles, procedimientos para mitigar el riesgo y gestionar la información de manera ordenada, parte del estudio del estado del arte, reveló que en el estado ecuatoriano no existen antecedentes documentados de que otras instituciones públicas hayan diseñado un plan estratégico de seguridad de la información basado en riesgos.

Conclusiones

Se pudo conocer la situación problémica de la institución mediante la aplicación de una evaluación de riesgos basada en la norma ISO/IEC 27005.

Mediante la aplicación de los controles segregados de la norma ISO 27002 y la aplicación de los instrumentos de investigación, se pudo definir un apropiado Plan Estratégico de Seguridad de la Información.

Para apalancar un adecuado Plan Estratégico de Seguridad de la Información es necesario definir adecuadamente políticas de seguridad informática y su alineación con los objetivos estratégicos de la institución.

Agradecimiento

El presente trabajo de investigación fue realizado bajo la supervisión del MsC. Juan Sebastián Grijalva a quien le agradezco por lograr que obtuviera una madurez profesional haciendo que sea capaz de resolver muchos problemas tecnológicos y de seguridad de la información.

Agradecer a mi familia a mi esposa y mis hijas quienes me apoyan todos los días haciendo que sea una persona capaz de cumplir los objetivos que me proponga y siendo un mejor profesional cada día.

Referencias

27005:2012, N. I.-I. (2017). *Instituto Ecuatoriano De Normalización* (Vol. 27006). Retrieved from http://www.normalizacion.gob.ec/wp-content/uploads/downloads/2014/NORMAS_2014/GAN/12092014/nte_inen_iso_iec_27006 extracto.pdf

Diéguez, M., Cares, C., & Cachero, C. (2017). Información Methodology for the Information Security Controls Selection. *2017 12th Iberian Conference on Information Systems and Technologies (CISTI)*, 1–6. https://doi.org/10.23919/CISTI.2017.7975811

Espinosa, D., Martínez, J., Amador, S., & Amador, S. (2014). Gestión del riesgo en la seguridad de la información con base en la Norma ISO/IEC 27005 de 2011, proponiendo una adaptación de la Metodología OCTAVE-S. Caso de estudio: proceso de inscripciones y admisiones en la división de admisión registro y control AC. *Ingenierías USBmed*, *5*(2), 33. https://doi.org/10.21500/20275846.309

Falconí Marco, R. L. (2010). Respeto hacia sí mismo y hacia los demás. Retrieved from http://bibdigital.epn.edu.ec

Freitas, V. De. (2009). Análisis y evaluación del riesgo de la información : caso de estudio Universidad Simón Bolívar Analysis and Risk Assessment of Information : Case Study Universidad Simon Bolivar, (1), 43–55.

Guzman, C. (2015). Diseño de un Sistema de Información para una Entidad Financiera de Segundo Piso.

Lozano Clave, M. (2017). Diseño De Un Plan Estratégico De Seguridad De Información (Pesi) Para Una Compañía Del Sector Asegurador.

Manuel Fernández Sánchez Mario Piattini Velthuis, C. (2012). *Modelo para el gobierno de las TIC basado en las normas ISO*.

MINTEL. (2017). No Title, *1*.

Nacional, U., & San, M. D. E. (2007). Gestión de seguridad de la información y los servicios críticos de las universidades : un estudio de tres casos en Lima Metropolitana.

Naranjo, D. (n.d.). – PROYECTO TÉCNICO –, 4–7.

Pallas, G., & Corti, M. (2009). Metodología de Implantación de un SGSI en grupos empresariales de relación jerárquica. *Fing.Edu.Uy*, 186. Retrieved from http://www.fing.edu.uy/inco/eventos/cibsi09/docs/Papers/CIBSI-Dia2-Sesion3(4).pdf

RamírezCastro, A., & OrtizBayona, Z. (2011). Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. *Ingeniería*, *16*(2), 56–66. Retrieved from http://revistas.udistrital.edu.co/ojs/index.php/reving/article/view/3833

Ryan, H., & Aguinaga, E. (2013). Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO / IEC 27001 : 2005 para una empresa de producción y comercialización de productos de consumo masivo.

Sandra, S. (2015). Análisis Y Diseño De Un Sistema De Gestión De Seguridad Informática En La Empresa

Aseguradora Suárez Padilla & Cía. Retrieved from http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3777/1/20904541.p df

Secretaria Nacional de Administración Pública. (2013). Acuerdo MInisterial 166-Esquema gubernamental de seguridad de la informacion EGSI, 1–47.

Siler, A. D. (2014). Full-Text.

Talabis, M., & Martin, J. (2012). Information Security Risk Assessment: Maintenance and Wrap Up. *Information Security Risk Assessments*, 233–250. https://doi.org/10.1016/B978-1-59-749735- 0.00008-7

Toinga, L. (2012). Escuela politécnica nacional, 150. Retrieved from http://bibdigital.epn.edu.ec/bitstream/15000/14623/1/CD-6793.pdf