Modelo de gestión de riesgos de ti para mejorar la gestión de seguridad de la información en la Universidad Nacional Toribio Rodríguez de Mendoza – Chachapoyas

Oscar Ñañez C.[1]
0000-0002-7840-3999

Fecha Recepción: 02 DIC 2020

Fecha Aceptación: 04 DIC2020

Resumen

El presente trabajo de investigación tiene como objetivo de elaborar un modelo de gestión de riesgos de TI basados en la norma ISO/IEC 27005 y metodología Magerit, para mejorar la gestión de seguridad de la información en la Universidad Nacional Toribio Rodríguez de Mendoza – Chachapoyas Perú.

Asimismo, este estudio consiste en desarrollar las actividades y tareas de las dos principales fases de un sistema de gestión de riesgos de TI, como son: la evaluación de los riesgos y el tratamiento de los mismos; para cada uno de los activos de TI que se tenían que protegerse, con la finalidad de asegurar una gestión adecuada de la seguridad de la información en los procesos académicos y administrativos identificados como críticos.

Palabras Claves: Modelo de Gestión, Riesgo de TI, Seguridad de la Metodología MAGERIT

Abstract

The purpose of this research work is to develop an IT risk management model based on the ISO / IEC 27005 standard and Magerit methodology, to improve information security management at the Toribio Rodríguez de Mendoza National University - Chachapoyas Peru.

Likewise, this study consists in developing the activities and tasks of the two main phases of an IT risk management system, such as: risk assessment and their treatment; for each of the IT assets that had to be protected, in order to ensure proper management of information security in academic and administrative processes identified as critical.

Keywords: *Management Model, IT Risk, MAGERIT Methodology*

Introducción

Este trabajo de investigación plantea una problemática administrativa siendo la falta de seguridad y la poca previsión respecto a los riesgos con la que cuentan sus activos de información. El resultado de todo ello es de no tener las medidas necesarias para mitigar estos riesgos puede llevar a la empresa a

[1] *Especialidad. Magister en Ingeniería de Sistemas de la EPG – UNPRG. oscar_nanez@hotmail.com*

pérdidas no solo de información, sino también económica.

Por lo tanto, la UNTRM actualmente no cuenta con Sistema de Gestión de Riesgos que le permita identificar todos los activos de información, asimismo no conoce la importancia de los activos de la información y por último no Identifica los posibles escenarios de riesgos,

Es por ello que se plantea una propuesta investigación donde pretende desarrollar un modelo de Gestión de riesgos de TI que les permita a los responsables de la seguridad de la información de la UNTRM identificar los elementos a considerar y la relación entre ellos, para facilitar la identificación, análisis, evaluación, tratamiento y monitoreo de los riesgos de TI. Para ello se plantea el desarrollo de una metodología, estructurada bajo los criterios definidos en la metodología MAGERIT v.3, las directrices de la norma internacional ISO 27005

Teniendo en cuenta las variables de investigación según Gómez, Pérez, Donoso y Herrera (2010) definen a la gestión de seguridad de la información como la característica de la Información que se logra mediante la adecuada combinación de políticas, procedimientos, estructura organización y herramientas especializadas a efectos que dicha información cumpla los criterios de confidencialidad, integridad y disponibilidad.

Asimismo, Espinoza (2013) define el Sistema de Gestión de Seguridad de Información como el concepto central sobre el que se construye ISO 27001. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

Por otro lado, Alexander (2011) lo define como una forma sistemática de administrar la información sensible de una institución, para que permanezca segura. Abarca a las personas, los procesos y las tecnologías de información. La forma total de la Seguridad de la información, y la integración de diferentes iniciativas de seguridad necesitan ser administradas para que cada elemento sea completamente efectivo. Aquí es donde entra el Sistema de Gestión de Seguridad de la Información que permite coordinar esfuerzos de seguridad con mayor efectividad.

Así, se tiene en cuenta la otra variable de estudio, en términos generales la gestión del riesgo se refiere a los principios y metodologías para la gestión eficaz del riesgo, mientras que gestionar el riesgo se refiere a la aplicación de estos principios y metodologías a riesgos particulares (Alexander, 2011).

Asimismo, es el proceso en el que se tratan los riesgos, para obtener un beneficio. Se centra en identificar y tratar riesgos, con el fin de añadir valor, aumentando la probabilidad de éxito o reduciendo la de fallo o incertidumbre. Debe ser un proceso continuo y de constante desarrollo, que se lleve a cabo en toda la estrategia, tratando los riesgos de actividades pasadas, presentes y futuras. Debe estar integrado en la cultura de la empresa, con políticas y programas dirigidos por la alta

dirección. Debe convertir la estrategia en objetivos tácticos, asignando responsabilidades a los empleados por la gestión del riesgo, promoviendo así la eficiencia operacional (Aliaga Flores, 2013)

Por otro lado, se pretende evaluar el modelo propuesto, en base a características de calidad establecidas en la ISO 25010. El modelo de calidad de la ISO 25010 establece un sistema para la evaluación de la calidad.

En el modelo de calidad de la ISO 25010 se determinan características de calidad que se deben tener en cuenta a la hora de evaluar las propiedades del modelo de gestión de riesgos TI propuesto. La calidad del modelo se puede interpretar como el grado en que dicho modelo satisface los requisitos de sus usuarios aportando de esta manera un valor. La población serán las personas que tienen la autoridad y la responsabilidad de la gestión de riesgos de TI en la UNTRM

Por lo tanto, la presente investigación está sistematizada en forma coherente, clara y sencilla; de tal manera que quien acceda a su estudio pueda comprenderlo, profundizar en su estudio y aplicarlo.

Está referido al desarrollo de la propuesta, presentación de los resultados y el análisis e interpretación de los resultados.

Por último, Se desarrolla el marco metodológico de la investigación y diseño de investigación, general y específicas; las variables con sus definiciones conceptual y operacional; la metodología empleada, describiendo el tipo de investigación y el diseño de la misma, método y técnicas con sus respectivos instrumentos de recolección de datos. El estudio realizado es de tipo propositiva; cuya población estuvo constituida a los líderes de la Universidad Nacional Toribio Rodríguez de Mendoza, y la responsabilidad de la gestión de riesgos de TI en la UNTRM

La Discusión de los resultados, se aplicaron después de un tratamiento estadístico.

Esperamos que el presente trabajo de investigación, contribuya como fuente de información para futuras generaciones

Metodología

La investigación fue desarrollada dentro del paradigma interpretativo, definida por Bodga y Taylor (1986) como aquella que busca entender los fenómenos sociales con una mirada desde el actor mismo, tomando en cuenta la subjetividad, asumida como el proceso por el cual se aprende a través de la observación. El estudio se trabajó con el

enfoque cualitativo que según Fernández (2014) se centra en la comprensión de fenómenos, a los cuales se les explora en un ambiente natural y desde la perspectiva del sujeto en relación con el contexto. Se asumió este enfoque, puesto que considera como un todo social a la vida misma, a la cual se le puede observar y analizar, usando en el proceso de la experiencia personal como un importante elemento que le permita al investigador acercarse a un contexto social. Se siguió rigurosamente las fases del método fenomenológico hermenéutico que implica aprehender la esencia del significado del afecto en la didáctica de la matemática; significado que es dado a partir de las opiniones y experiencias de los docentes sustentada por Manen (2003).

Resultados

Tabla N° 24. Análisis de brechas POST

Los documentos necesarios SGSI son: política SGSI, manual SGSI, procedimiento de gestión de riesgos, procedimiento de gestión de incidentes y vulnerabilidades, procedimiento de gestión de usuarios, procedimiento de control de accesos, procedimientos disciplinarios de seguridad, procedimiento para cese de personal, procedimiento para ingreso de personal, política sobre seguridad física y ambiental, procedimientos de la operación de sistemas, procedimientos para el monitoreo del trabajo de terceros, políticas sobre la gestión de la capacidad de procesamiento, procedimiento para la adquisición, desarrollo y mantenimiento de sistemas, procedimientos de respaldo.

Tabla N° 27. Identificación de expertos para la valoración del modelo de gestión de riesgos de TI basados en la norma ISO/IEC 27005 y metodología Magerit propuesto.

Aplicando el formato de encuesta que se muestra en el Anexo N° 4, se obtuvieron las valoraciones de cada uno de los expertos para cada uno de los criterios considerados para validar el modelo de gestión de riesgos de TI basado en la norma ISO/IEC 27005

Discusión

De la investigación se desprende una política de seguridad de información que sea desplegada a todos los colaboradores, proveedores y terceros involucrados en los procesos de tecnología. Alexander (2011) lo define como una forma sistemática de administrar la información sensible de una institución, para que permanezca segura. Abarca a las personas, los procesos y las tecnologías de información. Espinoza (2013) define el Sistema de Gestión de Seguridad de Información como el concepto central sobre el que se construye ISO 27001. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático,

documentado y conocido por toda la organización.

Por último, se logró elaborar un procedimiento, adecuando el marco de referencia de la metodología MagerIT, para desarrollar las actividades y tareas de las dos principales fases de un sistema de gestión de riesgos de TI, como son: la evaluación de los riesgos y el tratamiento de los mismos; para cada uno de los activos de TI que se tenían que protegerse, con la finalidad de asegurar una gestión adecuada de la seguridad de la información en los procesos académicos y administrativos identificados como críticos.

Conclusiones

Se contó con trabajo colaborativo tanto el personal responsable y la autoridad en la gestión de la seguridad de la información de la universidad, se elaboraron las tablas que permitieron definir el apetito de riesgo que tienen la institución.

La propuesta de apetito de riesgos está basada en la definición de tablas que determinan los niveles de impacto y frecuencia de exposición al riesgo. Estas tablas fueron utilizadas para determinar los niveles de exposición al riesgo tolerable y no tolerable.

Asimismo, con los indicadores KRI (indicadores claves de riesgo) se logró determinar la mejora en la gestión de los riesgos, en base a los resultados obtenidos en las fases de análisis y tratamiento de los riesgos que están propuestos en el modelo. A través de estos indicadores se identificó las brechas de seguridad, llegando a concluir que el modelo, permite disminuir estas brechas.

Por último, el modelo de gestión de riesgos de TI propuesto fue validado a través de un procedimiento de valoración por el juicio de tres expertos, calificando la coherencia, claridad, pertinencia y suficiencia del modelo, llegando a obtener, en cada uno de las categorías mencionadas, valores que sobrepasan la media en una escala de cinco niveles. Por tanto, el modelo es calificado como favorable para la gestión de riesgos de TI en la universidad.

Referencias Bibliográficas

Aguirre Freire, D. S., & Palacios Cruz, J. C. (2014). Evaluación técnica de seguridades del data center del municipio de Quito según las normas ISO/IEC 27001:2005 SGSI e ISO/IEC 27002:2005. Ecuador: Universidad de las fuerzas armadas ESPE, Sede SANGOLQUI.

Aguirre Mollehuanca, D. A. (2014). Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A. tesis pregrado. Lima: Pontificia Universidad Católica del Perú.

Alexander, A. (2011). Análisis y Evaluación del Riesgo de Información: Un Caso en la Banca Análisis y Evaluación del Riesgo de Información: Un Caso en la Banca. CENTRUM - Centro de Negocios, Pontificia Universidad Católica del Perú.

Aliaga Flores, L. (2013) Implementación De Un Sistema De Gestión De Seguridad De La Información Aplicando NTP ISO/IEC 27001:2014 En El Sector Hospitalario. Universidad Privada Norbert Wiener. Lima

Bodga, T. y Taylor, W. (1986) Sistema de Gestión de Información para una institución financiera. Tesis para optar el título de ingeniero informático

BSI Group México. (s/a). Pasando de ISO/IEC 27001:2005 a ISO/IEC 27001:2013. ISO/IEC 27001 – Gestión de Seguridad de la Información – Guía de Transición.

Carrasco, C. A. (2010). Impacto del riesgo en el gobierno de las tecnologías de Información y comunicación en la gestión empresarial industrial del siglo XXI. Lima-Perú.

Caviedes Sanabria, F., & Prado Urrego, B. A. (2012). Modelo unificado para identificación y valoración de los riesgos de los activos de información en una organización. Santiago de Cali.

Concha Huacoto, N. E. (2005). Propuesta para implantar CMMI en una empresa con multiples unidades desarrolladoras de software. Tesis pregrado. Lima: Universidad Nacioanl Mayor de San Marcos.

Condori Alejo, H. I. (2012). Un Modelo de Evaluación de Factores Críticos de Éxito en la Implementación de la Seguridad en Sistemas de Información para determinar su influencia en la intención del usuario. tesis postgrado. Lima: Universidad Inca Garcilaso de la Vega.

De la Cruz Guerrero, C. W., & Vasquez Montenegro, J. C. (2008). Elaboración y aplicación de un Sistema de Gestión de la Seguridad de la Información (SGSI) para la realidad Tecnólogica de la USAT. tesis pregrado. Chiclayo: Universidad Catolica Santo Toribio de Mogrovejo.

Eleven Paths. (23 de febrero de 2016). Gestión de Incidentes. Obtenido de http://blog.elevenpaths.com/2016/02/gestion-de-incidentes-i.html

Espinoza Aguinaga, H. R. (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. Tesis pregrado. Lima: Pontificia Universidad Católica del Perú.

Fernández, D. (2014) Gestión de Riesgos Tecnológicos basados en la ISO 31000 e ISO 27005.Colombia

Gómez, R., Pérez, D. H., Donoso, Y., & Herrera, A. (2010). Metodología y gobierno de la gestión de riesgos de tecnologías de la información. Revista de Ingeniería, 0(31), 109. https://doi.org/10.16924/riua.v0i31.217

Manen, O. (2003). Lecciones aprendidas en la implementación de sistemas nacionales de información de salud interoperables: una revisión sistemática. Rev Panam Salud Pública. 2014;35(5/6):415–23