Journal de Ciencia e Ingeniería

Journal de Ciencia e Ingeniería, Vol.6, No.1, Agosto de 2014, pp. 28-36
Investigación - Gestión de Riesgos

Definición de una Metodología de Gestión de Riesgos para Entidades del Sector Público Bajo el Estándar ISO 27001

Definition of a risk Management Methodology for Public Sector Entities Under the Standard ISO 27001

Carlos Mario Arteaga Pacheco [a] ⋆, Paula Andrea Villa Sánchez [a], Martha Isabel Ladino Aricapa [a]

[a] *Grupo de investigación en Telecomunicaciones Nyquist, Programa de Ingeniería de Sistemas y Computación, Universidad Tecnológica de Pereira, Colombia*

Recibido: 13/2/2014; revisado: 2/3/2014; aceptado: 28/4/2014.

C.M. Arteaga Pacheco, P.A Villa Sánchez, M.I. Ladino Aricapa: Definición de una Metodología de Gestión de Riesgos para Entidades del Sector Público Bajo el Estándar ISO 27001. Jou.Cie.Ing. **6** (1): 28-36, 2014. ISSN 2145-2628.

Resumen

Durante el proceso de Planificación para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), es necesario el uso de un modelo o metodología para la definición y análisis de riesgos asociados a los activos de información para la construcción del Mapa de Riesgos de dichos activos, que sirva como instrumento guía para emprender acciones tendientes a la reducción de la afectación a la integridad, confidencialidad y disponibilidad de la información. A partir del análisis comparativo y la evaluación de los diferentes modelos y metodologías disponibles en el medio para la evaluación de riesgos, se elaboró una metodología que cumpla con los requerimientos de la Norma ISO 27001 y se adapte a las características propias de las entidades públicas.

***Palabras Claves*:** ISO 27005, ISO 27001 metodología, riesgo, sistema de gestión de seguridad de la información (SGSI), vulnerabilidad, amenaza, entidades públicas.

Abstract

During the planning process for the implementation an Information Security Management System (ISMS) using a model or methodology for the definition and analysis of risks associated with information assets to build the necessary map risks of such assets, which serve as an instrument guide for action aimed at reducing the effect on the integrity, confidentiality and availability of information. From the comparative analysis and evaluation of the different models and methodologies available in the environment for risk assessment; methodology is built to achieve compliance with the requirements of ISO 27001 and suits the characteristics of public entities.

***Keywords*:** ISO 27005, ISO 27001, methodology, risk, system information security management system (ISMS), threat, vulnerability, public entities.

⋆ arteagam@utp.edu.co

1. Introducción

Para la fase de Planeación de un Sistema de Gestión de Seguridad de la Información, es necesario utilizar una Metodología de Gestión del Riesgo, que permita aplicar un conjunto de procesos, técnicas y herramientas en torno a los riesgos de los activos de información para identificarlos, valorarlos, tratarlos y controlarlos. Ante la existencia de diversas metodologías, es necesario determinar cuál es la que mejor se adapta a las necesidades particulares de la organización, o si en su defecto, es necesaria la formulación de una nueva que permita una aplicación más ajustada a las realidades del sector organizacional. Para determinar la Metodología de Gestión de Riesgos a utilizar en entidades del sector público, se realiza un análisis comparativo entre las disponibles en la región, incluyendo como parámetro fundamental las necesidades planteadas por el Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea 2.0 del gobierno colombiano. Adicionalmente, observar las características particulares de las entidades del sector público colombiano, las cuales deben cumplir con la normatividad vigente y obtener las certificaciones necesarias.

Al experimentar incidentes con la información en una organización, se generan impactos negativos que afectan de en menor o mayor grado las operaciones de negocio, lo cual se traduce generalmente en pérdidas económicas; que en las entidades públicas son llamadas detrimentos patrimoniales y generalmente conducen a demandas, investigaciones y sanciones.

Para mitigar estos impactos sobre la organización, se requiere implementar un Sistema de Gestión de Riesgos de Activos de Información, que mediante un con junto de actividades permita conocer cuál es el inventario de los activos relacionados con la información, qué agentes externos (amenazas y riesgos) e internos (debilidades y vulnerabilidades), son los que afectan o pueden afectar estos activos.

La implementación del Sistema de Gestión de Riesgos de Activos de Información permitirá realizar de manera disciplinada y sistemática el análisis y evaluación del riesgo de los Activos de Información identificados para determinar cuáles deben ser protegidos por generar un alto impacto y cuáles son los que la entidad está dispuesta a asumir.

El presente Artículo resume el procedimiento seguido y los resultados obtenidos por el equipo de trabajo durante la búsqueda de la respuesta a la pregunta que surge como consecuencia inmediata de lo discutido hasta el momento, cuál es la metodología que permite realizar un análisis y gestión del riesgo de Activos de Información que dé cumplimiento a los requisitos de la ISO 27001 y tenga plena aplicabilidad en entidades del sector público colombiano?.

2. Metodologías y Modelos de Gestión de Riesgos

La investigación sobre metodologías existentes para la gestión de Riesgos de Activos en las organizaciones permitió identificar y seleccionar ocho (8) metodologías y modelos:

3. Análisis Comparativo de Modelos y Metodologías de Gestión de Riesgos de Seguridad de la Información

Se consolidó el criterio de un grupo de expertos en el área de Gestión de Riesgos, considerando la información que se requiere para evaluar el cumplimiento de los requisitos de la Norma ISO 27001 [1, 2], obteniendo el siguiente listado mínimo de ítems como punto de partida para el análisis:

- Alcance
- Aplicación
- Objetivos
- Beneficios
- Fases de la metodología
- Proceso de gestión utilizado
- Instrumentos
- Elementos principales
- Compatibilidad con otros sistemas de gestión
- Antigüedad
- Cambios significativos con respecto a versiones anteriores (Si aplica)
- Limitaciones
- Complejidad en la aplicación
- Requerimientos de capacitación del personal involucrado
- Disponibilidad de bibliografía
- Casos de demostración disponibles

Se realizó un análisis comparativo de las metodologías a partir de los criterios definidos [3], lo cual se resume en la tabla 3.

Tabla 1. Metodologías identificadas para Gestión de Riesgos.

No	Metodología / Método	Comentario
1	COBIT 5	Es una guía de mejores prácticas presentado como framework, dirigida al control y supervisión de tecnología de la información (TI). Mantenido por ISACA (en inglés: Information Systems Audit and Control Association) y el IT Governance Institute (ITGI, en inglés: IT Governance Institute) [4, 5].
2	Metodología de gestión de riesgos de gobierno en línea v2.0 [6].	ANEXO 6: METODOLOGÍA DE GESTIÓN DEL RIESGO - MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA LA ESTRATEGIA DE PROBIEREN EN LÍNEA 2.0. Coordinación de Investigación, Políticas y Evaluación Programa Agenda de Conectividad Estrategia de Gobierno en línea. Bogotá, D.C., Diciembre de 2001.
3	COSO	Gestión de Riesgos Corporativos - Marco Integrado Técnicas de Aplicación. committee of Sponsoring Organizations of the Treadway Commission (COSO). Septiembre 2004.
4	PMBOK ® [7]	Guía de los Fundamentos para la Dirección de Proyectos. 4ª Edición. Capítulo 11 - Gestión de los Riesgos del Proyecto.
5	Norma ISO 31000	GESTIÓN DEL RIESGO.PRINCIPIOS Y DIRECTRICES. Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC). Bogotá, D.C. 2011 [8].
6	Norma ISO 27005 [9]	Norma ISO/IEC 27005:2008. Tecnología de la Información. Técnicas de Seguridad - Gestión del Riesgo en la Seguridad de la Información. 2ª Edición, 1 de Junio de 2011.
7	MAGERIT [10]	Versión 2. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.
8	Guía para la Gestión de Riesgos de TI [11]	Guía de administración de riesgos de seguridad de Microsoft. Microsoft Corporation. 2004.

Los siguientes ítems fueron considerados como informativos:

- Antigüedad
- Cambios significativos con respecto a versiones anteriores
- Requerimientos de capacitación del personal involucrado.
- Disponibilidad de bibliografía
- Casos de demostración

Para todos los ítems analizados se evidenció que el modelo propuesto por la ISO 27005 cumple en gran medida con los criterios establecidos por el grupo de expertos para la elección de la metodología o proceso a seguir.

Para la comparación de los ocho (8) modelos y metodologías de Gestión del Riesgo se elaboró el resumen de los principales elementos en términos de ventajas y desventajas.

A partir del comparativo de ventajas y desventajas, se continúo con la confrontación de cada uno de los ítems de las metodologías para analizar las características de la metodología o el método frente a lo que se requiere aplicar en entidades del sector público.

Los expertos definieron el siguiente conjunto de criterios que debería cumplir la metodología o método de gestión del riesgo:

El análisis final se presenta en resumen en la siguiente tabla, no se consideraron los criterios informativos.

La Norma Técnica Colombiana ISO/IEC 27005 cumple con los criterios definidos en el análisis comparati-

vo [3], lo cual es la justificación para utilizar el modelo de procesos definido en dicha norma, en las Entidades del Estado.

Tabla 2. Resultado comparación de metodologías de gestión de riesgos según los criterios evaluados en cada una.

Criterio	Modelo ó Metodología
Elementos principales: ▪ Compatibilidad con SGC y SGR de la organización ▪ Debe considerar un enfoque sistemático y estructurado ▪ Debe contener guías e instrumentos	▪ La ISO 31000 ▪ La ISO 27005 ▪ La guía de gobierno en línea ▪ La guía de Microsoft
Compatibilidad con otros sistemas de gestión: debe ser compatible con ISO 9000 ó ISO 27000 ó ISO 31000	Cobit5 con ISO 31000 [12] e ISO 9000 e ISO 27000 La ISO 31000 con ISO 9000 La ISO 27005 con ISO 9000 e ISO 27000 MAGERIT con ISO 27005
Limitaciones: Las limitaciones deben ser subsanables sin complicaciones.	La ISO 27005, es un conjunto de directrices para la gestión de los riesgos, esto hace que requiera ser formulada como una metodología
Complejidad en la aplicación: Facilidad de implementación	Metodología de Microsoft
Elementos principales: Compatibilidad con SGC y SGR de la organización. Debe considerar un enfoque sistemático y estructurado. Debe contener guías e instrumentos.	La ISO 31000 La ISO 27005 [9] La guía de gobierno en línea La guía de Microsoft
Compatibilidad con otros sistemas de gestión: debe ser compatible con ISO 9000 ó ISO 27000 ó ISO 31000	Cobit5 [13] con ISO 31000 e ISO 9000 e ISO 27000 La ISO 31000 con ISO 9000 La ISO 27005 con ISO 9000 e ISO 27000 Magerit con ISO 27005
Limitaciones: Las limitaciones deben ser subsanables sin complicaciones.	La ISO 27005, es un conjunto de directrices para la gestión de los riesgos, esto hace que requiera ser formulada como una metodología.

Su compatibilidad con la ISO 9000 e ISO 31000 permitirá su adherencia a los procesos de la Organización y a Sistemas de Gestión del Riesgo.

Esta norma proporciona un conjunto de directrices para la gestión del riesgo en seguridad de la información, sin embargo no brinda una metodología específica para la gestión del riesgo. Corresponde a la organización definir su enfoque de acuerdo a sus necesidades y el contexto de aplicación.

Por lo anterior, se procedió a definir una Metodología de Gestión de Riesgos de Activos de Información, como un conjunto de seis procesos, acorde con la estructura de Procesos de Gestión del Riesgo de la ISO 27005, complementando el enfoque con otras metodologías como la de Gobierno en Línea [6] y la Guía de Microsoft [11], para facilitar su aplicación y subsanar la limitación del modelo de la ISO 27005 [9].

Con fundamento en el conjunto de procesos de la metodología, se procedió a definir un proceso de aplicación de la misma, considerando de igual forma, la aplicación de actividades de la Guía de Microsoft y Gobierno en Línea.

Tabla 3. Criterios definidos por expertos.

Con relación a:	Criterios
Al alcance:	Identificación de los procesos de la organización donde se encuentren los activos de información.
Al ámbito de aplicación	Se requiere aplicación sobre los procesos que traten activos de información sensibles para el cumplimiento de la misión de la organización.
Los objetivos	La metodología de Gestión del Riesgo definida debe garantizar la valoración de activos de información considerando las vulnerabilidades y amenazas, según lo requerido en: TECHNICAL REPORT ISO/IEC TR 13335-3.
Los beneficios	Asegurar la información. Facilidad de implementación. Cumplimiento de regulación vigente.
Las fases de la metodología	Compatibilidad con el Sistema de Gestión de Calidad (SGC) y con el Sistema de Gestión del Riesgo (SGR) de la organización.
Al proceso de gestión utilizados	Compatibilidad con SGC y SGR de la organización.
Los instrumentos	Existencia de instrumentos y fácil aplicabilidad.
Los elementos principales	Compatibilidad con SGC y SGR de la organización. Debe considerar un enfoque sistemático y estructurado.Debe contener guías e instrumentos.
La compatibilidad con otros Sistemas de Gestión:	Debe ser compatible con ISO 9000 ó ISO 27000 ó ISO 31000.
Las limitaciones	Las limitaciones deben ser subsanables sin complicaciones.
La complejidad en la aplicación	Facilidad de implementación

Figura 1. Conjunto de procesos de la metodología de gestión de riesgos.

Los pasos definidos son:

Tabla 4. Procesos para la aplicación de la metodología.

Proceso	Paso
Establecimiento del contexto	1. Levantamiento de información inicial 2. Establecer criterios básicos para la Gestión del Riesgo 3. Definir alcance y límites de la Gestión del Riesgo 4. Establecer una organización para la operación del SGRSI
Valoración del Riesgo	5. Identificar Activos de Información 6. Identificar las amenazas y las vulnerabilidades 7. Identificar los controles existentes 8. Identificar consecuencias 9. Valorar las consecuencias 10. Valorar los incidentes 11. Determinar el nivel de estimación del riesgo 12. Evaluar el riesgo
Tratamiento del Riesgo	13. Seleccionar controles
Aceptación de Riesgo	14. Aceptar el riesgo
Comunicación de Riesgo	15. Comunicar el riesgo
Monitoreo y Revisión del Riesgo	16. Monitorear y revisar los riesgos

Tabla 5. Activos de información por categoría.

Categoría		Conteo	%
AI	Activo de Información	370	84,3 %
AF	Activo de Físico	38	8.7 %
S	Servicios	20	4,6 %
AS	Activo de Software	11	2,5 %
P	Personas	0	0,0 %
TOTAL	ACTIVOS	439	100,0 %

Estos pasos fueron aplicados en una entidad pública, para validar la Metodología a través de la aplicación en un caso de estudio que se describe a continuación.

4. Caso de Estudio en Entidad Pública

A continuación se describe brevemente las actividades que se llevaron a cabo para la aplicación de la metodología.

4.1. *Proceso: Establecimiento del Contexto*

PASO 1: **Levantamiento de información inicial**

1. Se recopiló información de los procesos y procedimientos de la empresa.
2. Se recopiló el inventario de activos de información catalogado por proceso o área, donde se indique el responsable y la ubicación de cada uno.
   a) Se consolidó la información en la tabla *Tabla de inventario de activos*.
   b) Si no existía el inventario en el Proceso, se realizó el levantamiento para catalogar los activos de información del Proceso tomando como insumo la *"tabla maestra de registros"*, *"la tabla de retención documental"* y *"las caracterizaciones de cada proceso"*.
   c) Para complementar la información suministrada, se realizó entrevistas a los líderes de proceso.
3. Se recopiló listado de líderes de procesos.
4. Se recopiló listado de áreas o dependencias.
5. Se recopiló organigrama de la organización.

El análisis de la información solicitada y las entrevistas realizadas permitieron:

- Hacer un estimativo del número total de activos de la empresa.
- Identificar las áreas de negocio de la empresa, las cuales están distribuidas por subprocesos.
- Identificar los líderes de subprocesos.
- Identificar los activos que pertenecen a cada subproceso
- Realizar el proceso para el tratamiento de cada activo.

PASO 2: **Establecer criterios básicos para la Gestión del Riesgo**

Se consolidó el total de Activos de Información bajo las categorías de la clasificación de la Guía de Gobierno en Línea.

El comité de seguridad de la información estableció los criterios básicos de seguridad de la información, con base en los que ya se encontraban definidos en el sistema General de Gestión del Riesgo.

PASO 3: **Definir alcance y límites de la Gestión del Riesgo**

En la ejecución de este paso se realizó la capacitación sobre la metodología de gestión de riesgos con los líderes de las áreas de proceso.

Para determinar el alcance de la Gestión de Riesgos en Seguridad de la Información y a su vez el alcance del Sistema de Gestión de Seguridad de la Información, se catalogaron los activos de información por cada proceso en la entidad, definiéndose que debían incluirse en primera instancia los procesos de mayor número de activos de información: proceso 1, proceso 2 y proceso 3, así como los dos procesos más sensibles: proceso 4 y proceso 5 (ver tabla 6), tomándose en el alcance un total de 227 activos de información, que equivalen al 52 % del total de activos de información. Este límite se sometió a consideración y aprobación por parte del comité de seguridad de la información.

Se propuso por parte de los Líderes de Proceso y algunos integrantes del Comité de Seguridad de la Información, establecer el límite para los activos cuya relevancia fuera "Crítica", "Muy importante¿ e "Importante", lo cual fue aprobado por el Comité de Seguridad de la Información en una reunión posterior. Finalmente se socializó el alcance acogido.

PASO 4: **Establecer una organización para la operación del SGRSI**

Durante este paso el Comité Directivo mediante Resolución definió la conformación del comité de seguridad de la información, el cual fue alineado con el Comité de Gobierno en Línea, para lo cual se asignaron las funciones a los integrantes.

4.2. *Proceso: Valoración de Riesgos*

PASO 5:**Identificar activos de información**

La identificación de activos de información se realizó en el paso 1, para así definir el alcance y valorar de manera más objetiva los activos a ser considerados en el SGSI.

Para la realización de los pasos 6, 8, 9, 10, 11, 12, 13, 14, 15 y 16 que se especifican a continuación, se confirmaron subgrupos de trabajo por cada uno de los procesos definidos en el alcance, de tal manera, que los Líderes de cada uno de estos subprocesos determinaran los riesgos y su tratamiento.

Para el paso 7, los Líderes de las áreas de los procesos se apoyaron en las personas encargadas del área de Tecnologías de la información, puesto que ellos son los encargados de administrar aspectos asociados a los controles del hardware y del software.

4.3. *Proceso: Valoración de Riesgos*

PASO 6: **Monitorear y revisar los riesgos**

Durante la ejecución de este proceso se identificaron 31 riesgos, para los cuales se definieron opciones de tratamiento de acuerdo a los criterios básicos definidos en el paso 2.

Tabla 6. Activos de Información por Categoría.

PROCESO AL CUAL PERTENECE	ACTIVOS DE INFORMACIÓN	%
Proceso 1	78	17,8 %
Proceso 2	66	15,0 %
Proceso 3	50	11,4 %
Subproceso 3.1	38	8,7 %
Subproceso 3.2	31	7,1 %
Subproceso 3.3	26	5,9 %
Subproceso 3.4	25	5,7 %
Subproceso 3.5	22	5,0 %
Subproceso 3.6	21	4,8 %
Proceso 4	20	4,6 %
Subproceso 4.1	16	3,6 %
Subproceso 4.2	15	3,4 %
Proceso 5	13	3,0 %
Subproceso 5.1	58	1,8 %
Subproceso 5.2	5	1,1 %
Subproceso 5.3	5	1,1, %
TOTAL	439	100 %

5. Conclusiones

La metodología de Gestión de Riesgos se definió como una estructura de seis procesos, los cuales están enmarcados en el ciclo de Deming: Planear, Hacer, Verificar y Actuar PHVA.

Los procesos de la Metodología de Riesgos están estructurados según el Sistema de Gestión de la Calidad de la organización, de la Norma ISO 31000 y en pro de cumplir con los objetivos de la Norma ISO 27001 [1] para alcanzar una futura certificación.

En la estructura de procesos definidos en la metodología de gestión de riesgos están incluidos doce (12) instrumentos como anexos que facilitan la ejecución de los procesos.

En el ejecución del paso a paso se identificó que era necesario inicialmente definir el inventario de activos para establecer el alcance y los límites del SGSI.

Se evidenció que la existencia de un Sistema de Gestión de Calidad y un Sistema de Gestión de Riesgos General en la empresa facilita la aplicación de la metodología de Gestión de Riesgos.

La aplicación de la metodología de Gestión de Riesgos permite que los líderes de los procesos participen y proporcionen la información necesaria para darle el tratamiento adecuado a los activos de la información.

El paso a paso de la metodología de la gestión de Riesgos permitió la aplicación de los instrumentos de una manera más sencilla para los involucrados en el proceso.

El resultado de la aplicación de la metodología de

Gestión de los Riesgos fue el insumo para definir la Política General de Seguridad de la Información y las asociadas a cada aspecto de la ISO 27001, así como los lineamientos.

El caso de estudio permitió validar la aplicabilidad de la Metodología Propuesta para la Gestión de Riesgos de activos de Información en entidades del Sector Público colombiano.

Recomendaciones

La aplicación de la Metodología de Gestión de Riesgos de Activos de Información Desarrollada, debe ir acompañada de un proceso pedagógico de formación a los funcionarios de la entidad, por tratarse de conceptos y términos relativamente nuevos en el ámbito organizacional.

Agradecimientos

Se agradece la participación de los funcionarios de la entidad para la ejecución de las actividades de la prueba piloto de la Metodología de Gestión de Riesgos de Activos de Información.

Referencias

[1] *Norma ISO/IEC 27001:2005 Tecnología de la Información – Técnicas de Seguridad de la Información – Requerimientos.*, 1 edition, 15 Oct 2005.

[2] Normas y estándares iso. en organización internacional para la estandarización.

[3] *Norma ISO/IEC 27005:2008. Tecnología de la Información. Técnicas de Seguridad - Gestión del Riesgo en la Seguridad de la Información.*, 2 edition, 1 Jun 2011.

[4] http://www.aec.es/web/guest/centro conocimiento/cobit. Coby web site.

[5] Sergio Sperat. Todo lo que usted quería saber de cobit 5 y no se animó a preguntar. http://estratega.org/site/todo-lo-que-usted-queria-saber-sobre-cobit-5-y-no-se-animo-a-preguntar/.

[6] *Normas Generales de Control Interno. Auditoria Interna de la Nación*, chapter Anéxo 6: Metodología de gestión del riesgo - modelo de seguridad de la información para la estrategia de gobierno en línea 2.0. Coordinación de Investigación, Políticas y Evaluación Programa Agenda de Conectividad Estrategia de Gobierno en línea, 2007.

[7] *PMBOK. Guía de los Fundamentos para la Dirección de Proyectos.*, chapter 11- Gestión de los Riesgos del Proyecto. 4 edition.

[8] Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC). *NTC-ISO 31000. Gestión del riesgo. principios y directrices.* Bogotá D.C., 2011.

[9] Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC). *NTC-ISO 27005. Tecnologías de la información. técnicas de seguridad. gestión del riesgo en la seguridad de la información.* Bogotá D.C., 2009.

[10] *MAGERIT –versión 2. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Guía I – Método*. Ministerio de Administraciones Públicas, Jun 2006.

[11] Microsoft Corporation. Guía de administración de riesgos de seguridad de microsoft, 2004.

[12] Alexandra Ramírez Castro. Riesgo tecnológico y su impacto para las organizaciones. parte ii: Gobierno de ti y riesgos.

[13] http://www.isaca.org/COBIT/Documents/COBIT5 Introduction-Spanish.ppt. Cobit 5 introducción.