risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Revista Ibérica de Sistemas y Tecnologías de Información

Recebido/Submission: 01/03/2017
Aceitação/Acceptance: 01/05/2017

Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000

Francisco Javier Valencia-Duque [1], Mauricio Orozco-Alzate [1]

fjvalenciad@unal.edu.co, morozcoa@unal.edu.co

[1] Universidad Nacional de Colombia – Sede Manizales - Departamento de Informática y Computación - Campus La Nubia, km 7 vía al Magdalena, Manizales, 170003 - Colombia.

DOI: 10.17013/risti.22.73–88

Resumen: Se propone una metodología de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la familia de normas de la ISO/IEC 27000, con énfasis en la interrelación de cuatro normas fundamentales a través de las cuales se desarrollan las actividades requeridas para cumplir con lo establecido en la ISO/IEC 27001, los controles de seguridad presentados en la ISO/IEC 27002, el esquema de riesgos de la ISO/IEC 27005 y los pasos recomendados en la ISO/IEC 27003. Se genera como resultado un proceso metodológico que da respuesta al *cómo* abordar un proyecto de este nivel de importancia en el contexto actual de las organizaciones y basado en estándares internacionales. Este proceso metodológico representa un aporte a los profesionales que emprenden esta labor, y que buscan un método para una implementación exitosa de un SGSI.

Palabras-clave: Seguridad de la Información, ISO/IEC 27000; SGSI, Riesgos de TI, Metodologías.

A methodology for implementing an information security management system based on the family of ISO/IEC 27000 standards

Abstract: A methodology for the implementation of an Information Security Management System (ISMS) based on the ISO/IEC 27000 family of standards is proposed, with an emphasis on the interrelationship of four fundamental standards which break down the activities to be developed in order to comply with the requirements established in the ISO/IEC 27001, the safety controls presented in the ISO/IEC 27002, the ISO/IEC 27005 risk scheme and the steps recommended in the ISO/IEC 27003. The result is a methodological process that explains how to face a project of this level of importance in the current context of organizations and based on international standards. This methodological process represents a contribution to the professionals who undertake this work, and who are looking for a method to carry out a successful implementation of an ~~ISMS~~.

Keywords*:* Information Security, ISO/IEC 27000, ISMS, IT Risks, Methodologies.

1. Introducción

Las Tecnologías de Información y Comunicaciones (TIC) son recursos esenciales para la productividad y competitividad de las organizaciones; sin embargo, como cualquier recurso, está sujeto a múltiples amenazas que se pueden materializar en riesgos, con múltiples consecuencias.

Hoy en día las amenazas tecnológicas son parte de nuestra cotidianeidad y más aún de la vida organizacional, las cuales van desde diversas formas de virus, pasando por los recientes ataques de *ransomware* hasta amenazas sofisticadas como los ataques día cero (en inglés, *zero-day attack*) lo cual requiere la implementación de controles que puedan ser gestionados a través de un adecuado enfoque de seguridad de la información.

La seguridad de la información es una disciplina asociada tradicionalmente a la gestión de TIC, cuyo propósito es mantener niveles aceptables de riesgo de la información organizacional y de los dispositivos tecnológicos que permiten su recolección, procesamiento, acceso, intercambio, almacenamiento, transformación y adecuada presentación. Ha sido definida por la norma ISO/IEC 27000 como la preservación de la confidencialidad, integridad y disponibilidad de la información (ISO/IEC, 2014).

La adopción temprana de la ISO 27001 en todo el mundo en comparación con otros estándares de gestión (Freixo & Rocha, 2014; Tunçalp, 2014), pone de manifiesto la importancia que ha tomado la seguridad de la información, lo cual se ratifica a partir del número de certificaciones otorgadas por la Organización Internacional para la Estandarización (ISO) en los últimos años, presentando un crecimiento exponencial, al pasar de un total de 5797 certificaciones en el año 2006, a 27536 en 2015, siendo Japón y el Reino Unido los países con mayor número de empresas certificadas, de acuerdo al último informe de la entidad (ISO, 2017). No obstante, las normas establecen el *deber ser*, y no la forma como se logra, de allí la importancia de establecer metodologías que permitan orientar a las organizaciones en la forma como se debe abordar este tipo de procesos, con el respaldo de las normas internacionales promulgadas para tal fin.

Este artículo propone una metodología para llevar a cabo la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), para lo cual parte de la diferenciación entre seguridad de la información y seguridad informática, seguido de una explicación de las principales normas de la familia ISO/IEC 27000 como base para la presentación de las cinco fases que hacen parte de la metodología de implementación basada en la ISO/IEC 27003:2010.

2. Seguridad de la información vs seguridad informática

Antes de abordar un enfoque metodológico para implementar un SGSI es necesario aclarar la diferencia entre seguridad informática y seguridad de la información, la cual radica en el tipo de recursos sobre los que actúa cada una. Mientras que la primera se enfoca en la tecnología propiamente dicha, i.e. en las infraestructuras tecnológicas que sirven para la gestión de la información en una organización, la segunda está relacionada con la información en sí misma, como activo estratégico de la organización. En este sentido las TIC son herramientas que permiten optimizar los procesos de gestión de la información en las organizaciones. El concepto de seguridad es el mismo, pero mientras la seguridad

informática desarrolla su función sobre todos los elementos técnicos que hacen parte de las TIC, la seguridad de la información actúa sobre la información como activo estratégico para la adecuada toma de decisiones empresariales en las organizaciones modernas.

Hasta antes que surgieran de forma masiva las TIC, el concepto predominante era el de seguridad de la información; sin embargo, con el advenimiento de las TIC y su nivel de dependencia por parte de las organizaciones y más aún, su nivel de dependencia para un adecuado tratamiento de la información, se ha pasado de pensar tan solo en la seguridad informática como fin, a pensar en su adecuada implementación como medio para obtener un SGSI que permita garantizar niveles adecuados de protección de la información empresarial como recurso vital para la función decisional, y el diseño de estrategias competitivas que diferencien una organización de otra. Desde esta perspectiva lo que persigue un SGSI es proteger la información como recurso valioso, para lo cual debe proteger de igual forma los diferentes medios a través de los cuales se genera, almacena, procesa, transmite, circula y transforma en un recurso útil para los negocios. Estos medios son las TIC en su conjunto.

3. Estándares de seguridad de la información

Uno de los requisitos para implementar un SGSI en una organización es conocer los estándares, su estructura y la relación existente entre cada uno de ellos.

Las normas para implementar un SGSI corresponden a la serie ISO/IEC 27000 publicadas por la ISO y la Comisión Electrotécnica Internacional (IEC), compuesta por aproximadamente 17 normas, clasificadas en cuatro categorías: *i*) La norma que contiene el vocabulario, contenido en la norma ISO/IEC 27000; *ii*) las normas de requerimientos, contenidos en la norma ISO/IEC 27001 y la norma ISO/IEC 27006; *iii*) las normas guía desarrolladas a través de 10 normas: ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005, ISO/IEC 27007, TR 27008, ISO/IEC 27013, ISO/IEC 27014, TR 27016, ISO/IEC 27032 y *iv*) las normas para sectores específicos, contenidas en las normas ISO/IEC 27010, ISO/IEC 27011, TR 27015 y TS 27017.

Figura 1 – Principales normas para implementar un SGSI basado en los estándares de la familia de normas ISO/IEC 27000

A pesar de la cantidad de normas de la serie ISO/IEC 27000, aquéllas que sirven de referente para la implementación de un SGSI en una organización se enmarcan en cuatro de ellas, como se puede observar en la figura 1.

3.1. Norma ISO/IEC 27001:2013

Norma denominada formalmente *Tecnología de información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requerimientos*, la cual especifica los requerimientos para el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora de un SGSI debidamente formalizado. El cumplimiento de los requerimientos de esta norma, permite que una organización pueda obtener la certificación internacional en ISO/IEC 27001.

3.2. Norma ISO/IEC 27002: 2013

Esta norma denominada formalmente como *Tecnología de información - Técnica de seguridad - Código de prácticas para controles de seguridad de la información* ha sido diseñada de acuerdo con ISO (2015) para ser usada en organizaciones que intentan: (a) seleccionar controles dentro de un proceso de implementación de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001; (b) implementar controles de seguridad de la información comúnmente aceptados; (c) Desarrollar sus propias guías de gestión de seguridad de la información.

La estructura de los controles de seguridad de la información se encuentra conformada por 14 dominios, 35 objetivos de control y 114 controles, los cuales se encuentran divididos entre controles organizacionales, controles técnicos y controles normativos, como se puede apreciar en la figura 2.

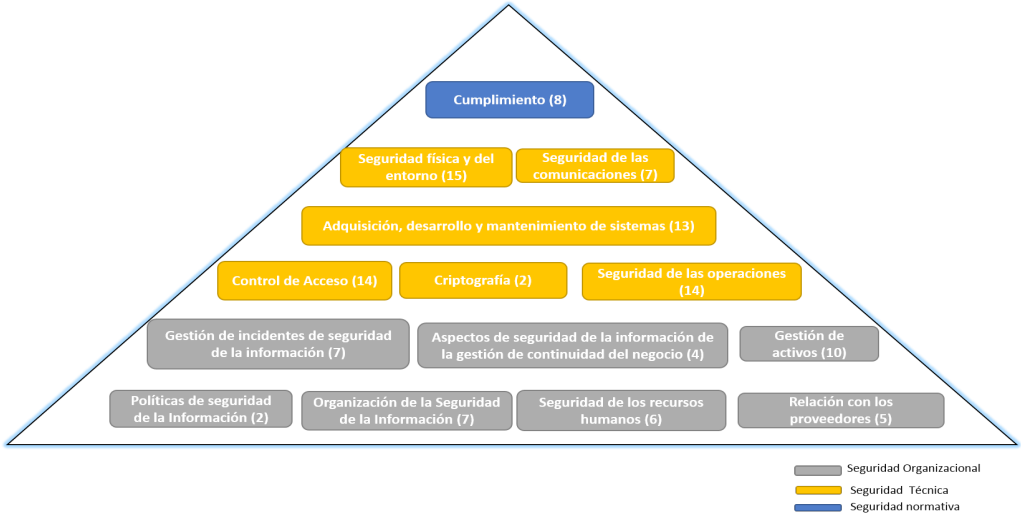

Figura 2 – Estructura de los controles de la norma ISO/IEC 27002

3.3. Norma ISO/IEC 27003:2010

Esta norma denominada formalmente como *Tecnología de información - Técnica de seguridad - Guía de implementación de un sistema de gestión de seguridad de la información* cuyo objetivo es el establecimiento de las especificaciones y diseño de un SGSI, la cual será el referente para esta propuesta metodológica.

3.4. Norma ISO/IEC 27005: 2008

Denominada formalmente como *Tecnología de la información - Técnicas de seguridad - Gestión del riesgo en la seguridad de la información* es la norma que proporciona directrices para la gestión del riesgo de la seguridad de la información, sin proporcionar metodologías específicas para tal fin. El componente de gestión del riesgo, es uno de los insumos esenciales para desarrollar un SGSI. Si bien existen múltiples marcos de referencia, en su mayoría presentan los mismos elementos.

4. Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información

Existen diversas formas de llevar a cabo una implementación de un SGSI en una organización, no obstante, para lograr cierto nivel de éxito y disminuir la incertidumbre en sus resultados, se debe adoptar un enfoque que permita abordar, desde una perspectiva sistémica, la forma de cumplir con los elementos que hacen parte de éste. El enfoque propuesto en este artículo está basado en la norma ISO/IEC 27003:2010 y se combinará con la experiencia de los autores en el tema.

La metodología contempla cinco (5) fases secuenciales, las cuales serán detalladas con la suficiente granularidad como para poder comprender los pasos a desarrollar no sólo desde el punto de vista conceptual sino metodológico, a partir de un proyecto que incorpore personas, tiempos y recursos así como el respaldo de la alta Dirección, como un requisito fundamental para cumplir los objetivos previstos.

Estas cinco fases con sus respectivas etapas están distribuidas en función de la norma ISO/IEC 27001, tal como se puede apreciar en la tabla 1 y cuyo cumplimiento es obligatorio, si se quiere cumplir con los requisitos exigidos para obtener la certificación internacional.

A continuación, se explicará en detalle cada una de estas fases, tratando de incorporar una serie de elementos prácticos que permitan poner en contexto su implementación.

4.1. Fase 1: Aprobación de la Dirección para iniciar el proyecto

Uno de los aspectos que se deben tener en cuenta y que no es a menudo claramente comprendido, es que un proyecto de SGSI no es un proyecto del área de Tecnologías de Información, es un proyecto organizacional y como tal requiere la aprobación y el apoyo de la Dirección para avanzar en su adecuada implementación. Para cumplir con este propósito se deben llevar a cabo las siguientes actividades:

Establecimiento de las prioridades de la organización para desarrollar un SGSI: Para llevar a cabo esta actividad es necesario conocer a fondo las prioridades que

Fases 27003:2010	Etapas	Numerales de la norma ISO/ IEC 27001:2013 relacionados
Obtener la aprobación de la Dirección para iniciar el proyecto	Establecimiento de las prioridades de la organización para desarrollar un SGSI	4.1. Conocimiento de la organización y de su contexto.
	Definir el alcance preliminar del SGSI	4.2. Comprensión de las necesidades y expectativas de las partes interesadas.
	Creación del plan del proyecto para ser aprobado por la Dirección	5.1. Liderazgo y compromiso 7.1. Recursos
Definir el alcance, los límites y la política del SGSI	Definir el alcance y los límites del SGSI	4.3. Determinación del alcance del sistema de gestión de seguridad de la información.
	Definir el alcance y los límites de las Tecnologías de Información y Comunicaciones	
	Definir el alcance y los límites físicos	
	Integrar cada alcance y los límites para obtener el alcance y los límites del SGSI	
	Desarrollar la política del SGSI y obtener la aprobación de la Dirección	5.1. Liderazgo y compromiso 5.2. Política 6.2. Objetivos de seguridad de la información y planes para lograrlos.
	Definición de roles, responsabilidades del SGSI	5.3. Roles, responsabilidades y autoridades en la organización. 7.2. Competencia 7.3. Toma de conciencia
Realizar el análisis de los requisitos de seguridad de la información	Definir los requisitos de seguridad de la información para el proceso SGSI	4.2. b) La organización debe determinar los requisitos de las partes interesadas pertinentes a la seguridad de la información.
	Identificar los activos dentro del alcance del SGSI	
	Realizar una evaluación de la seguridad de la información	6.1.2. Valoración de riesgos de seguridad de la información.
Realizar la valoración de riesgos y planificar el tratamiento de riesgos	Realizar la valoración de riesgos	6.1.2. Valoración de riesgos de seguridad de la información.
	Seleccionar los objetivos de control y los controles	6.1.3. Tratamiento de riesgos de la seguridad de la información. 6.2. Objetivos de seguridad de la información y planes para lograrlo.
	Obtener la autorización de la Dirección para implementar y operar el SGSI	5.1. Liderazgo y compromiso

Diseñar el SGSI	Diseñar la seguridad de la información de la organización	7.4. Comunicación
	Diseñar la seguridad física y de las Tecnologías de Información y Comunicaciones	7.5. Información documentada 8.1. Planificación y control operacional
	Diseñar la seguridad específica de un SGSI	8.2. Valoración de riesgos de seguridad de la información.
	Producir el plan del proyecto final del SGSI	8.3. Tratamiento de riesgos de seguridad de la información. 9.1. Seguimiento, medición, análisis y evaluación 9.2. Auditoría interna 9.3. Revisión por la Dirección

Tabla 1 – Fases de implementación de un SGSI y su relación con los numerales de la norma ISO/IEC 27001:2013

tiene la organización para implementar un SGSI, para lo cual se recomienda tener en cuenta los siguientes elementos:

Objetivos estratégicos de la organización: este elemento permitirá determinar la forma como un SGSI puede aportar a los diferentes objetivos de la organización y justificar aún más su necesidad como parte de la estrategia organizacional. Una vez identificados los objetivos estratégicos a los cuales podría aportar el SGSI, se pueden establecer las líneas de negocio y los procesos involucrados que dependen de estos objetivos estratégicos.

Requisitos normativos o de terceros relacionados con la seguridad de la información: es necesario identificar los requerimientos normativos que tenga la entidad, o los requerimientos que en materia de información se tengan de terceros y que requieran cumplir con criterios de confidencialidad, integridad y disponibilidad de la información. Estos requisitos son fundamentales para complementar la necesidad de justificar un SGSI.

Sistemas de gestión existentes: con el fin de poder aprovechar la base instalada con que cuenta la organización en relación a otras normas de sistemas de gestión ya incorporadas en la organización, es necesario identificarlas si se tiene en cuenta que por lo general todas las normas de gestión basadas en las normas ISO cuentan con algunos elementos estructurales idénticos y como tal pueden ser compatibles con los requerimientos establecidos en la norma ISO/IEC 27001:2013. Se ha podido establecer de acuerdo a (Mesquida, Mas, Feliu, & Arcilla, 2014) que en la mayoría de los casos, cuando una empresa decide implantar una norma de gestión de seguridad de la información, ya ha tenido otras experiencias en la incorporación de sistema de gestión basados en ISO. Es importante que el SGSI sea parte de la estructura de gestión de la organización, y se

incorpore como parte de los procesos, en aquellas actividades que requieren adecuados niveles de protección de la información.

Definir el alcance preliminar del SGSI: El punto de partida para desarrollar un SGSI es definir qué se quiere proteger y con base en ello se determina de manera preliminar el alcance. De acuerdo a lo establecido en la norma ISO/IEC 27003, el alcance preliminar incluye un resumen de los requisitos establecidos por la Dirección y las obligaciones impuestas externamente a la organización.

Creación del plan del proyecto para ser aprobado por la Dirección: Si bien la incorporación de un SGSI en la organización es una tarea permanente, el primer paso para impulsar su diseño e implementación parte de la elaboración de un proyecto que permita definir con certeza los tiempos, recursos y personal requerido, utilizando para ello las diferentes herramientas de gestión de proyectos existentes en el mercado.

Una vez formulado el proyecto es necesario e importante involucrar a la alta Dirección de la organización, si se tiene en cuenta que es allí donde inicia el proyecto y es ella, en últimas, la que autoriza la implementación y operación del SGSI. Adicionalmente, es allí donde se aprueba el presupuesto del plan de mitigación de riesgos resultante del análisis de riesgos.

Es necesario que la Dirección proporcione evidencias de su compromiso con los procesos y actividades que están involucrados en el establecimiento, implantación, operación, monitoreo, evaluación, mantenimiento y mejora permanente del SGSI de acuerdo con la cláusula 5 de la norma ISO 27001:2013; estableciendo la política de seguridad de la información, fijando los objetivos, asignando los papeles y las responsabilidades, la comunicación de la importancia de la gestión de seguridad de la información para el negocio, la provisión de recursos para el SGSI y la decisión sobre el nivel aceptable del riesgo.

4.2. Fase 2: Definir el alcance, los límites y la política del SGSI

Esta fase contempla los siguientes elementos:

Definición del alcance: La importancia que tiene el establecimiento del alcance está fundamentada en que permite delimitar el proceso de gestión de riesgos y, por ende, pone foco a todo el proceso de implementación del SGSI.

El alcance se establece en función del negocio y/o en función de su ubicación en el caso de aquellas entidades que cuentan con varias sedes y puede ir desde un proceso, un conjunto de procesos, una sede, un servicio o un conjunto de servicios y debe ser adecuadamente definido para evitar ambigüedades, teniendo presente que su definición no conlleve a un proyecto inalcanzable en términos de tiempo y recursos.

Se recomienda establecer el alcance, desarrollando previamente matrices que permitan cruzar los procesos de la organización con los requisitos, o con los dominios de la norma ISO 27001:2013 relacionados en el anexo A y que son aplicables a la organización.

El producto final del alcance, por lo general, es un párrafo que resume lo que se está protegiendo en la organización y hace parte del documento de certificación entregado a aquellas entidades que logran cumplir con los requisitos exigidos.

Definición de la política y objetivos de seguridad: De acuerdo a Diaz (2010) la política de seguridad refleja lo que la organización quiere hacer con respecto a la seguridad de la información, los objetivos que pretende conseguir, contemplando los requisitos legales y reglamentarios aplicables y teniendo en cuenta el compromiso de la Dirección para conseguirlos.

Una política es una directriz que ayuda al cumplimiento de los objetivos, definida en función del alcance, y se encuentra contemplada como el primer control de la norma ISO/IEC 27002. Es importante tener en cuenta que la política general de seguridad de la información es una sola, y a partir de allí se pueden definir las diferentes políticas específicas en los diferentes niveles, tales como: política de acceso, política de uso de dispositivos móviles, política de *backups*, entre otros.

En cuanto a los objetivos de seguridad, es importante delimitar los dos tipos de objetivos que contempla un SGSI: los objetivos generales del sistema y los objetivos de control resultantes del proceso de análisis y valoración de riesgos. Al menos en esta primera parte se deben definir los objetivos generales que busca la implementación del SGSI, articulándolos con las políticas y dentro del alcance previsto.

Aprobación de la Dirección: Una de las formas de demostrar el apoyo de la Dirección de manera inicial, es la aprobación que ella da a las políticas y objetivos del SGSI dentro del alcance. De allí que el numeral 5.1. Literal a) de la norma ISO/IEC 27001:2013 establece, como parte del compromiso de la Dirección, el aseguramiento que ésta hace del establecimiento de la política y los objetivos de la seguridad de la información de modo que estos sean compatibles con la dirección estratégica de la organización.

4.3. Fase 3: Análisis de los requisitos de seguridad de la información

De acuerdo a lo establecido en la norma ISO/IEC 27003:2010 para establecer los requisitos de seguridad de la información se deben tener en cuenta cinco (5) elementos: Identificar (a) los activos de información importantes; (b) la visión de la organización y sus efectos sobre los requisitos futuros de procesamiento de información; (c) las formas actuales de procesamiento de información (aplicaciones, redes, la ubicación de las actividades y recursos de TI); (d) requisitos legales, reglamentarios, obligaciones contractuales, normas de la industria, acuerdos con clientes y proveedores, condiciones de pólizas de seguros, etc.; (e) el nivel de toma de conciencia sobre seguridad de la información y los requisitos de formación y educación en seguridad.

Estos requisitos justifican la necesidad de contar con un SGSI en la organización.

Identificar los activos dentro del alcance del SGSI: Las organizaciones cuentan con una gran cantidad y variedad de activos tecnológicos, y tratar de establecer y clasificar estos activos puede ser una tarea de grandes proporciones, sobre todo en aquellas grandes organizaciones, ya que es probable que existan terabytes de datos electrónicos, almacenes de documentos y miles de personas y dispositivos que hacen parte de los activos tecnológicos (ISACA, 2012). Los activos en el contexto del SGSI, según la norma ISO/IEC 13335-1:2002, son cualquier activo de información físico o lógico que tiene valor para la organización.

La norma ISO/IEC 27005 diferencia dos tipos de activos: primarios y de soporte. Los activos primarios son los procesos de negocio y la información, mientras que los activos de soporte, son aquellos de los cuales dependen los activos primarios y se clasifican en: hardware, software, redes, personal, ubicación y estructura de la organización.

La Dirección General de Modernización Administrativa Procedimientos e Impulso de la Administración Electrónica (2012) a través de MAGERIT establece una clasificación basada en capas tecnológicas interdependientes, teniendo presente que existen relaciones entre activos, formando grafos, a través de los cuales se puede observar el nivel de dependencia entre los diferentes activos tecnológicos.

Es necesario tener en cuenta que el valor de los activos se concentra generalmente en unos pocos, en especial en aquellos activos terminales (información, servicios, procesos) dadas las relaciones de dependencia que existen entre los activos primarios o terminales y los activos de soporte (Jiménez-martín, Vicente, & Mateos, 2015).

Se deben identificar y clasificar los activos de acuerdo a los requerimientos de seguridad y el nivel de criticidad para el negocio, así como establecer quién es el propietario de ese activo y quien debería ser el responsable de su seguridad (Pallas, 2009).

4.4. Fase 4: Valoración de riesgos y planificar el tratamiento de riesgos

Sin duda éste es el eje principal del SGSI, cuyo principal referente es la norma ISO/IEC 27005, no obstante, existen otros modelos que pueden ser utilizados para tal fin, entre los que se destacan: OCTAVE, CRAMM, NIST SP 800-30, MAGERIT, MEHARI, FAIR, RISK FOR COBIT 5.0. Al respecto se debe tener en cuenta:

Establecimiento de contexto: Esta fase contempla la preparación de los diferentes elementos que requiere el proceso de gestión de riesgos de seguridad de la información, partiendo del contexto, alcance, políticas, objetivos y parámetros de evaluación del riesgo.

Para llevar a cabo la actividad de evaluación se requiere el establecimiento de parámetros para evaluar los riesgos, los cuales deben ser racionales y fáciles de utilizar a lo largo del proceso de implementación del SGSI. Estos parámetros de referencia son los siguientes: parámetros de probabilidad, parámetros de impacto, vulnerabilidad y criterios de aceptación del riesgo.

Parámetros de probabilidad: Debe establecerse una tabla de frecuencias de la posible ocurrencia de las amenazas, con los niveles requeridos de acuerdo a las necesidades de la organización. Generalmente, se utilizan tablas con un rango de entre tres (3) y cinco (5) niveles. A cada nivel se le asigna un valor de referencia en una escala lineal, cuyo único requisito es que a mayor frecuencia dicho valor sea más alto. A cada nivel se le asigna un nombre que facilite su aplicación y adicionalmente se establecen criterios de valoración basados en número de veces que ha ocurrido o puede llegar a ocurrir, por lo general en el periodo de un año.

Parámetros de impacto: La gravedad de una amenaza no solo está en función de la cantidad de dinero que se pierde, sino en cómo los diferentes eventos que surgen en la organización y que están relacionados con la información pueden llegar a afectarla en su conjunto o en algunos procesos o a ciertas áreas.

Los parámetros de impacto se definen en función de las consecuencias que podría tener cualquier amenaza sobre la información o los activos de información en lo relacionado con confidencialidad, integridad y disponibilidad, tal como se ha explicado en los apartados anteriores.

Determinación de la vulnerabilidad: Para determinar qué tan importante es el riesgo, se ha establecido una nueva medida para estimar el impacto que una amenaza podría tener sobre la organización. Esta medida establece cuán grave sería para la organización que una amenaza ocurriera y afectara la información empresarial en términos de confidencialidad, integridad y disponibilidad. Esta medida genérica se conoce como *vulnerabilidad*, y corresponde a la sensibilidad de la organización frente a la posible materialización de una amenaza sobre la información empresarial**.**

La vulnerabilidad se mide en términos porcentuales y en función de los dos parámetros definidos previamente (probabilidad e impacto), y para ello se utiliza la siguiente formula: $V_X=(P \times I)/ \max (P \times I)$; Donde V_X es la vulnerabilidad del escenario de riesgo *X*, *P* es la probabilidad de ocurrencia e *I* es el impacto.

Criterios de aceptabilidad del riesgo: Los criterios de aceptación de riesgo permiten establecer el apetito de riesgo que tiene la organización y corresponde a los parámetros que define una organización para determinar si un riesgo es aceptable.

La determinación por parte de la organización de lo que es suficientemente seguro, es lo que delimita el nivel de seguridad de la empresa y los principales recursos y esfuerzos a desarrollar para mantenerse en este estado.

La mayor dificultad que existe para determinar las condiciones de seguridad de una organización, se fundamenta en el hecho de establecer los parámetros de aceptabilidad del riesgo, debido a la coincidencia de múltiples intereses, así como la evaluación hecha por personas con diferentes niveles de conocimientos, experiencia y "emotividad", lo que genera diversas percepciones sobre el mismo (Duque, 2017). Con el fin de compatibilizar todos los intereses existentes en la organización, es necesario que el equipo del SGSI en compañía de la alta dirección, determine la aceptabilidad del riesgo en forma coherente (Vanegas & Pardo, 2014).

Valoración del riesgo: La valoración del riesgo, de acuerdo a lo establecido en la norma ISO/IEC 27005:2009 contempla tres fases: identificación de los escenarios de riesgo, estimación del riesgo y evaluación del riesgo.

Identificación de escenarios de riesgo: El propósito de la identificación de riesgos es determinar qué podría suceder que cause una pérdida potencial, y llegar a comprender el cómo, dónde y por qué podría ocurrir esta pérdida (ICONTEC, 2009).

Si partimos del concepto de riesgo, tal como lo plantea la norma ISO/IEC 27000, como la incertidumbre sobre los objetivos, dicha incertidumbre se materializa a través de la identificación de los eventos que pueden llevar al incumplimiento de objetivos, estos eventos son tradicionalmente definidos como amenazas. Algunos ejemplos de amenazas se pueden observar en las encuestas y estudios de seguridad de la información que cada año elaboran diferentes entidades tales como CISCO, IBM, Deloitte, Ernst & Young, PwC, entre otros.

Una buena práctica para delimitar las amenazas específicas que tiene una organización es la construcción de un catálogo de amenazas que permita a los responsables identificar aquéllas que en su concepto se podrían materializar. Entre los referentes para tal fin se encuentran MAGERIT, el repositorio de vulnerabilidades del gobierno de los Estados Unidos y el repositorio de vulnerabilidades del Instituto de Ingeniería de Software (SEI).

La exposición de un recurso de información a una amenaza específica configura la "Unidad de Análisis Básica", y recibe el nombre de ESCENARIO DE RIESGO. La construcción de los escenarios de riesgo se realiza en función de las amenazas que pueden llegar a afectar a cualquier activo identificado dentro del alcance del SGSI.

ESCENARIO DE RIESGO= AMENAZA F (ACTIVO DE INFORMACIÓN)

Estimación del riesgo: Para estimar el riesgo, se pueden llevar a cabo análisis cualitativo, semicuantitativo o cuantitativo, o bien, una combinación de los tres (Shameli-Sendi, Aghababaei-Barzegar, & Cheriet, 2016). En cualquier caso, el tipo de análisis que se lleve a cabo debe ser congruente con los criterios desarrollados en el establecimiento del contexto. Como se mencionó en párrafos anteriores, para estimar el riesgo se acudirá a la estimación de la vulnerabilidad: en este caso la vulnerabilidad inherente y la vulnerabilidad residual, entendida la primera como la estimación de la vulnerabilidad, sin tener en cuenta los controles existentes, mientras que la segunda representa la estimación de la vulnerabilidad, teniendo en cuenta el efecto que tienen los controles sobre la disminución de la probabilidad o el impacto.

Evaluación del riesgo: La evaluación del riesgo consiste en realizar una comparación de las vulnerabilidades resultantes de cada riesgo y confrontarlas contra el nivel de aceptación de riesgo. De acuerdo con este concepto, deberán existir dos tipos de evaluaciones: antes de controles y después de controles, acorde a la estimación resultante en la fase anterior.

Los resultados arrojados de la evaluación de riesgos permiten diseñar mapas de riesgos, o mapas de calor, informes de vulnerabilidad por cada criterio de seguridad de la información y diversos indicadores que permiten monitorear el nivel de avance en la gestión del riesgo.

Tratamiento del riesgo: La fase de tratamiento de riesgos establece las acciones a desarrollar, a través de controles propuestos, para lograr llevar el riesgo a un nivel aceptable en la organización. Para ello se deben priorizar los riesgos residuales en función de los criterios de aceptabilidad, siendo prioritarios aquellos que se encuentran en el más alto nivel de vulnerabilidad.

Es importante tener en cuenta que la elaboración del plan de tratamiento de riesgos requiere un análisis de costo-beneficio de los controles a implementar y los techos presupuestales asignados para su elaboración, de allí la importancia de priorizar aquellos escenarios de riesgo que son más críticos para la organización.

Para su tratamiento se encuentran diversas opciones, las cuales han sido clasificadas por la norma ISO/IEC 27005 en cuatro alternativas: reducción del riesgo, retención del riesgo, evitar el riesgo, transferencia del riesgo.

Un plan de tratamiento de riesgos, por lo general contempla la siguiente estructura: escenario de riesgo, riesgo residual, alternativa de tratamiento, controles a implementar, responsable de su implementación (rol), valor estimado, fechas estimadas de implementación, efecto esperado del control en función de la disminución de la probabilidad o impacto, riesgo residual esperado después del plan de mitigación.

Numeral ISO/IEC 27001:2013		**Documentación**
4.3	*Determinación del alcance del SGSI*	El alcance debe estar disponible como información documentada
5.2	*Política de seguridad*	e) La política de seguridad debe estar disponible como información documentada
6.1.2.	*Valoración de riesgos de seguridad de la información*	Información documentada acerca del proceso de valoración de riesgos de la seguridad de la información
6.1.3	*Tratamiento de riesgos de seguridad de la información*	Información documentada acerca del proceso de tratamiento de los riesgos de seguridad de la información
6.1.3	*Declaración de aplicabilidad*	d) Declaración de aplicabilidad
6.2.	*Objetivos de seguridad de la información y planes para lograrlos*	Objetivos de la seguridad de la información
7.2	*Competencia*	Evidencia de la competencia de las personas relacionadas con la seguridad de la información
7.5.	*Información documentada*	b) La que la empresa ha determinado que es necesaria para la eficacia del SGSI
7.5.3	*Control de la información documentada*	La información documentada de origen externo
8.1	*Planificación y control operacional*	Información documentada para tener confianza de que los procesos se han llevado a cabo de acuerdo a lo planificado
8.2.	*Valoración de la seguridad de la información*	Resultados de las valoraciones de riesgos de la seguridad de la información
8.3	*Tratamiento de riesgos de seguridad de la información*	Resultados de los tratamientos de riesgos de la seguridad de la información
9.1	*Seguimiento, medición, análisis y evaluación*	Evidencia de los resultados del monitoreo y de la medición
9.2	*Auditoría interna*	g) conservar la información documentada como evidencia de la implementación del programa de auditoría y de los resultados de ésta.
9.3	*Revisión por la dirección*	Evidencia de los resultados de la revisión por la Dirección
10.1	*No conformidades y acciones correctivas*	Naturaleza de las no conformidades y cualquier acción posterior tomada
10.1	*No conformidades y acciones correctivas*	Resultados de cualquier acción correctiva

Tabla 2 – Resumen de la información documentada que debe tener un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013.

4.5. Fase 5: Diseñar el SGSI

El diseño del SGSI contempla básicamente tres componentes: La documentación que debe tener el sistema, la implementación de los controles previstos en el plan de tratamiento de riesgos y el monitoreo constante de la seguridad de la información.

Documentación del sistema: La información documentada que debe tener un SGSI comprende los requisitos contemplados en la norma ISO/IEC 27001, los cuales surgen a partir de la implementación de sus diferentes fases. Un resumen de la información a documentar como parte del SGSI se muestra en la tabla 2.

Implementar el plan de tratamiento de riesgos: La implementación del plan de tratamiento de riesgos aprobado por la alta dirección con los recursos asignados para tal fin, y el mantenimiento de los controles existentes, es lo que permite garantizar niveles aceptables de seguridad de la información en la organización.

De allí que debe existir un monitoreo permanente de los controles y de los nuevos escenarios de riesgos que surgen para mantener un SGSI pertinente y ajustado a la realidad de la organización.

Monitoreo de la seguridad de la información: Tal como lo establece el numeral 9, de la norma ISO/IEC 27001:2013, la evaluación del desempeño del SGSI se realiza a través de la supervisión, medición, análisis y evaluación del sistema; las auditorías periódicas y la revisión por la Dirección.

La supervisión, medición, análisis y evaluación del SGSI se realiza, por lo general, a través de la definición de indicadores. Estos indicadores son comúnmente desarrollados a nivel general del SGSI, a nivel de indicadores de gestión de riesgos y de los indicadores que permiten evaluar la eficacia y eficiencia de los controles que hacen parte de la declaración de aplicabilidad definida para el sistema.

En lo relacionado con las auditorías al SGSI existen tres (3) normas específicas que deben ser tenidas en cuenta al momento de desarrollar un proceso de auditoría: las normas ISO 19011:2011, ISO/IEC 27007:2011 e ISO/IEC TR-27008.

Por último, la revisión de la dirección corresponde a la alta Dirección, con el fin de asegurar la suficiencia del sistema para dar respuesta a los objetivos y la eficacia en su implementación. Esta revisión se desarrolla por lo general cada año y está basado en las mediciones y las auditorías internas desarrolladas durante el periodo.

5. Conclusiones

La cantidad de normas con que cuenta actualmente la familia ISO/IEC 27000 para llevar a cabo la implementación de un sistema de gestión de seguridad de la información, pone de manifiesto una complejidad adicional al proceso de desarrollo de un sistema de gestión de seguridad de la información. El presente trabajo aporta en la construcción de un proceso metodológico, a partir de la interrelación de cuatro de las principales normas que la conforman, allanando el camino para emprender un proyecto de este tipo y dar respuesta de esta forma a una necesidad sentida de la comunidad profesional de desarrollar metodologías ajustadas a los estándares internacionales, y en contexto con la organización. En futuras investigaciones, se espera aplicar la metodología a

organizaciones gubernamentales colombianas para dar cumplimiento a las diferentes regulaciones existentes actualmente.

Agradecimientos

Este artículo es producto de la investigación "Diseño de un modelo integrado de aseguramiento de Tecnologías de Información y Comunicaciones, basado en estándares internacionales" con código Hermes 32050 financiado por la Universidad Nacional de Colombia.

Referencias

Diaz, A. (2010). Sistema de Gestión de la Seguridad de la Información. *Revista Calidad*, (IV), 18–20.

Dirección General de Modernización Administrativa Procedimientos e Impulso de la Administración Electrónica. (2012). *MAGERIT - versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Mètodo*. Madrid: Ministerio de Hacienda y Administraciones Pùblicas, Ed.

Duque, A. C. (2017). *Metodología para la gestión de riesgos. Como integrar la seguridad a los objetivos estratégicos de los negocios de una manera costo-beneficiosa*. Retrieved April 10, 2017, from http://www.ridsso.com/documentos/muro/207_1469148692_57916e1488c74.pdf

Freixo, J., & Rocha, Á. (2014). Arquitetura de informação de suporte à gestão da qualidade em unidades hospitalares. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informaçã*o, (14), 1-15. http://dx.doi.org/10.17013/risti.14.1-15.

ICONTEC. (2009). *Norma Técnica Colombiana. NTC-ISO/IEC 27005. Tecnología de Información. Técnicas de Seguridad. Gestión del riesgo en la seguridad de la información*. Retrieved from https://tienda.icontec.org/wp-content/uploads/pdfs/NTC-ISO-IEC27005.pdf.

ISACA. (2012). *Manual de Preparación del examen CISM 2013*, Illinois: ISACA.

ISO. (2015). I*SO/IEC 27002:2013. Information technology — Security techniques — Code of practice for information security controls*. Retrieved March 17, 2015, from http://www.iso.org/iso/catalogue_detail?csnumber=54533

ISO. (2017). *ISO Survey 2015*. Retrieved March 15, 2017, from https://www.iso.org/the-iso-survey.html

ISO/IEC. (2014). *INTERNATIONAL STANDARD ISO / IEC 27000. Information technology — Security techniques — Information security management systems — Overview and vocabulary* (Vol. 2014). ISO/IEC

Jiménez-Martín, A., Vicente, E., & Mateos, A. (2015). Selección de salvaguardas en gestión del riesgo en sistemas de la información: un enfoque borroso. *RISTI - Revista Ibérica de Sistemas E Tecnologias de Informação*, (15), 83–100. http://doi.org/10.17013/risti.15.83-100

Mesquida, A. L., Mas, A., Feliu, T. S., & Arcilla, M. (2014). Integración de estándares de gestión de TI mediante MIN-ITs. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, *1*(E1), 31–45. http://doi.org/10.4304/risti.e1.31-45

Pallas, M. G., & Corti E. (2009). *Metodología de Implantación de un SGSI en un grupo empresarial jerárquico*. Retrieved from http://www.criptored.upm.es/cibsi/cibsi2009/docs/Papers/CIBSI-Dia2-Sesion3(4).pdf

Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of Information Security Risk Assessment (ISRA). *Computers & Security*, *57*, 14–30. http://doi.org/http://dx.doi.org/10.1016/j.cose.2015.11.001

Tunçalp, D. (2014). Diffusion and Adoption of Information Security Management Standards Across Countries and Industries. *Journal of Global Information Technology Management*, *17*, 221–227. http://doi.org/10.1080/1097198X.2014.982454

Vanegas, A., & Pardo, C. J. (2014). Hacia un modelo para la gestión de riesgos de TI en MiPyMEs : MOGRIT. *Revista S&T*, *12*(30), 35–48.