

GESTIÓN DEL RIESGO BASADO EN ISO/IEC 27005:2009 – ISO/IEC 31000:2011 ISO/IEC 28000:2008

Velasco Cortes, Ricardo Adolfo
ingevelascortes@hotmail.com
Universidad Piloto de Colombia

Abstract—This paper presents a summary of the main methodologies for risk treatment in the field of information security and shows the steps for risk management proposed by each methodology. It refers to three of the most commonly used methodologies for risk management: "ISO/IEC 31000, ISO/IEC 27005:2009 and MARGERIT" and makes an approach of how to apply the best practices of each in the risk management projects in organizations.

Resumen—Este Artículo presenta un resumen de las principales metodologías para el tratamiento del riesgo en el campo de la seguridad de la información y muestra las fases para la administración del riesgo que propone cada metodología. Hace referencia a tres de las metodologías más usadas para la administración de riesgos: "MARGERIT" [1], "ISO/IEC 31000 (Risk management) [2] e ISO/IEC 27005:2009 (Information security risk management) [3], y hace un planteamiento de cómo aplicar las mejores prácticas de cada una en los proyectos de gestión de riesgo de las organizaciones.

Palabras clave: Riesgo, Activo, Amenaza, Vulnerabilidad, Probabilidad, Control, Escenario.

I. INTRODUCCIÓN

El uso de las tecnologías de la información se ha incrementado sustancialmente en las organizaciones, a tal grado que dichas tecnologías prácticamente se han hecho indispensables para la operación de las organizaciones, independiente de la naturaleza y actividad de las mismas, por tal motivo la constante evolución de las organizaciones y sus crecientes necesidades demandan innovación tecnológica que les permita ser competitivas y alcanzar sus objetivos de negocio.

Inevitablemente la innovación tecnológica trae consigo riesgos que amenazan con impactar las infraestructuras tecnológicas, y por tanto a la organización; estos riesgos asociados se intensifican

y transforman, por lo cual se hace necesario evaluar y adaptar constantemente los métodos de procesamiento de la información y medios tecnológicos utilizados para preservar y proteger la información de los procesos críticos de la organización.

El riesgo originado por el uso de plataformas tecnológicas incide de forma indirecta sobre las metas y objetivos de la organización. Por esta razón las interrupciones, fallas, pérdida de disponibilidad, integridad y confidencialidad derivadas del uso de tecnología de la información puede implicar pérdidas significativas en las organizaciones, (financieras, multas o acciones legales, afectación de la imagen de la organización y causar afectación a nivel operativo y estratégico).

El desarrollo y uso de metodologías integradas en la gestión de riesgos es de vital importancia, para minimizar el impacto que puede causar la materialización de amenazas que afectan las propiedades que protege la seguridad de la información "Confidencialidad, Integridad y Disponibilidad".

En la actualidad existen varias metodologías para gestión de riesgos, el desarrollo y propósito del presente artículo se enfocará en "MARGERIT" [1], "ISO/IEC 31000:2011 (Risk management) [2], ISO/IEC 27005:2009 (Information security risk management) [3] e ISO/IEC 28000:2008 (Gestión de la seguridad en la cadena de suministro), dichas metodologías proveen lineamientos generales, lo cual en muchas ocasiones se hace necesario ajustar la metodología a las necesidades del negocio para alcanzar de forma más eficiente y eficaz los aspectos de seguridad requeridos.

El objetivo principal de este artículo es integrar las mejores prácticas en la gestión de riesgos de las metodologías mencionadas, la iniciativa plantea una metodología integrada más eficiente y ágil. Con el propósito de mostrar los beneficios de la iniciativa, presentaré primero una descripción general de los

aspectos más relevantes de cada metodología y las fases que la componen, luego desarrollaré el planteamiento de la metodología integral y presentaré las conclusiones.

II. MARGERIT

Metodología española promovida por el Ministerio de Administraciones Públicas de España y desarrollada por el Consejo Superior de Administración Electrónica (CSAE), para la gestión y análisis de riesgos de los sistemas de información que en sus tres libros “Método”, “Catalogo de elementos” y “Guía de técnicas” sirve como fuente de revisión de definiciones y lo correspondiente a la estimación de riesgos.

Margerit implementa el Proceso de Gestión de Riesgos, dentro de un marco de trabajo para la toma de decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

Las diferentes metodologías de riesgo persiguen la aproximación más acertada sobre los riesgos a los que está expuesta la información, soportados por los procesos, en este caso sobre los sistemas TIC y la seguridad de la información a través de guías informales, aproximaciones metódicas y herramientas de soporte, en busca de estandarizar el análisis de riesgos para saber cuán seguros (o inseguros) son los sistemas y no incurrir en falsos positivos que conlleven a sentir seguridad por desconocimiento.

Objetivos

- Concienciar a los responsables de la información en las organizaciones acerca de la existencia de riesgos y de la necesidad de gestionarlos.
- Establecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
- Planificar el tratamiento oportuno para mantener los riesgos bajo control.
- Preparar a la organización para procesos de evaluación, auditoría, certificación o acreditación.[1]

Fases Margerit [1]

1. Caracterización de activos
 - a. Identificación de los activos

El objetivo es identificar los activos que componen el sistema determinando sus características, atributos y la clasificación de los mismos en los tipos definidos así:

- Inventario de datos manejados por el sistema.
- Inventario de servicios prestados por el sistema.
- Procesos de negocio.
- Diagramas de uso.
- Diagramas de flujo de datos.
- Inventarios de equipamiento lógico.
- Inventarios de equipamiento físico.
- Locales y sedes de la organización.
- Caracterización funcional de los puestos de trabajo.

- b. Determinar dependencia entre activos.

Los activos esenciales son la información y los servicios que prestan, se debe determinar la dependencia entre activos de acuerdo a la propagación de su valor, enfocado a los requisitos de seguridad, su dependencia se registrará entonces por la Confidencialidad, la Integridad o la Disponibilidad.

- c. Valoración de los activos:

La valoración de los activos debe ser medida teniendo en cuenta la Confidencialidad, la Integridad y la Disponibilidad.

2. Caracterización de amenazas

- Identificación de amenazas
- Valoración de amenazas (probabilidad de ocurrencia), la probabilidad de ocurrencia se debe medir a través de escalas.

3. Caracterización de salvaguardas

- Identificación de salvaguardas pertinentes.
- Valoración de salvaguardas

4. Estimación del estado del riesgo

- Estimación del impacto
La estimación del impacto se debe medir a través de escalas que determinen en qué grado se ve afectado el activo por la materialización de la amenaza.
- Estimación del riesgo.
La estimación del riesgo está determinada por el resultado de la conjugación de la probabilidad x el impacto.

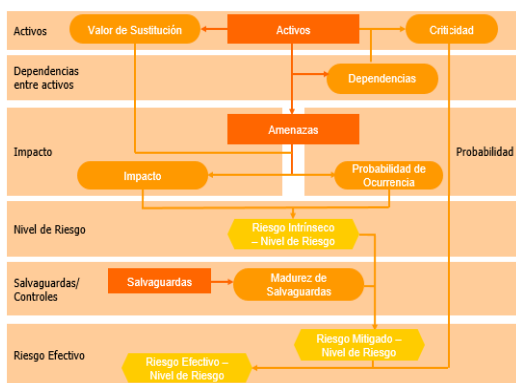


Fig.1 Fases Metodología Margerit, tomado de INTECO [4]

III. ISO/IEC 31000:2011 – GESTIÓN DE RIESGOS

Todas las actividades de una organización están sometidas permanente a una serie de amenazas, lo cual las hace altamente vulnerables, comprometiendo su estabilidad, ya sea través de accidentes, acciones deliberadas como ataques o las amenazas propias del negocio [2].

Las organizaciones han tratado estos riesgos mediante estrategias de reacción y soluciones puntuales. Sin embargo, la experiencia ha demostrado que los elementos que conforman los riesgos y los factores que determinan el impacto de sus consecuencias sobre un sistema, son los mismos que intervienen para todos los riesgos en una organización. Por esta razón, la tendencia moderna es utilizar un enfoque integral de manejo de los mismos conocido como “Risk Management Enterprise” (ERM), con el fin de evaluar, administrar y comunicar estos riesgos de una manera integral, basados en los objetivos estratégicos de la organización.

La gestión integral de riesgos ha tomado impulso en los últimos años, especialmente a partir de la década de los noventa, lo que ha conllevado la aparición de “Modelos de Gestión de Riesgos”, algunos de ellos de carácter más específico, como por ejemplo: COSO, ISO 14000, ISO 22000, OHSAS, etc. y otros de carácter más global como la norma AS/NZS 4630, ISO 28000 o la presente norma ISO 31000 [5].

La norma ISO/IEC 31000:2011 recomienda que las organizaciones desarrollen, implementen y mejoren continuamente un marco de referencia, cuyo propósito sea integrar el proceso para la gestión del riesgo en los procesos globales de gobierno, estrategia y planificación, gestión, procesos, políticas, valores y cultura de la organización.

La metodología propuesta por ISO/IEC 31000:2011 se resume en tres ejes estratégicos:

- Principios para la gestión del riesgo.
- Estructura para la gestión del riesgo.
- Procesos de gestión del riesgo.

Principios básicos para la gestión del riesgo ISO/IEC 31000:2011.

- a. Crea valor. Contribuye a la consecución de objetivos así como la mejora de aspectos tales como la seguridad y salud laboral, cumplimiento legal y normativo, protección ambiental, etc.
- b. Está integrada en los procesos de una organización. No debe ser entendida como una actividad aislada sino como parte de las actividades y procesos principales de una organización.
- c. Forma parte de la toma de decisiones. La gestión del riesgo ayuda a la toma de decisiones evaluando la información sobre las distintas alternativas.
- d. Trata explícitamente la incertidumbre. La gestión del riesgo trata aquellos aspectos de la toma de decisiones que son inciertos, la naturaleza de esa incertidumbre y como puede tratarse.
- e. Es sistemática, estructurada y adecuada. Contribuye a la eficiencia y, consecuentemente, a la obtención de resultados fiables.
- f. Está basada en la mejor información disponible. Los inputs del proceso de gestión del riesgo están basados en fuentes de información como la experiencia, la observación, las previsiones y la opinión de expertos.
- g. Está hecha a medida. La gestión del riesgo está alineada con el contexto externo e interno de la organización y con su perfil de riesgo.
- h. Tiene en cuenta factores humanos y culturales. Reconoce la capacidad, percepción e intenciones de la gente, tanto externa como interna, que puede facilitar o dificultar la consecución de los objetivos de la organización.
- i. Es transparente e inclusiva. La apropiada y oportuna participación de los grupos de interés (stakeholders) y, en particular, de los responsables a todos los niveles, asegura que la gestión del riesgo permanece relevante y actualizada.
- j. Es dinámica, iterativa y sensible al cambio. La organización debe velar para que la

gestión del riesgo detecte y responda a los cambios de la empresa.

- k. Facilita la mejora continua de la organización. Las organizaciones deberían desarrollar e implementar estrategias para mejorar continuamente, tanto en la gestión del riesgo como en cualquier otro aspecto de la organización.

Estructura ISO/IEC 31000:2011.

La diversidad, complejidad y naturaleza de los riesgos puede ser de muy densa, por lo que éste estándar internacional desarrollado por la ISO (International Organization for Standardization) propone unas pautas genéricas sobre cómo gestionar los riesgos de forma sistemática y transparente [2].

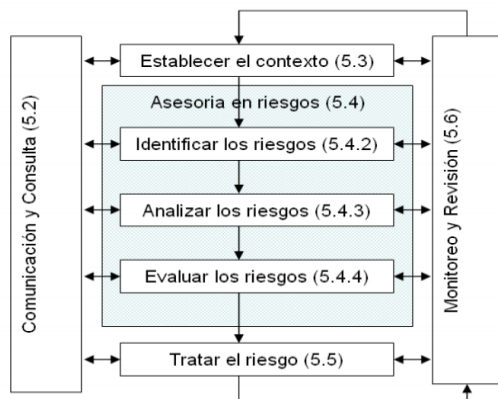


Fig. 2 Estructura ISO/IEC 31000, tomado de la norma ISO/IEC 31000:2011 [2]

El diseño y la implantación de la gestión de riesgos dependerán de las diversas necesidades de cada organización, de sus objetivos concretos, contexto, estructura, operaciones, procesos operativos, proyectos, servicios.

La relación entre los tres ejes estratégicos de gestión, los principios, la estructura de soporte y el proceso de gestión del riesgo, son la clave para una efectiva gestión de los riesgos.

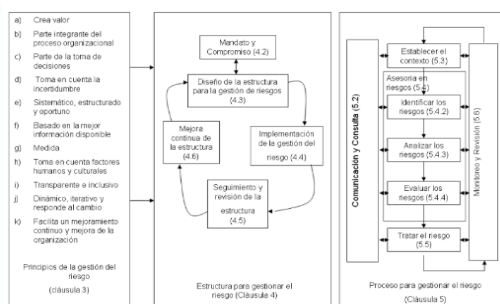


Fig. 3 Relación entre los 3 ejes estratégicos, tomado de la norma ISO/IEC 31000:2011 [2]

IV. ISO/IEC 27005:2009 – GESTIÓN DE RIESGOS

El estándar ISO/IEC 27005 coincide en buena parte de los elementos especificados en BS 7799-3, pero toma referencias adicionales de otros estándares reconocidos como el estándar "AS/NZS 4360:2004, Risk Management", no obstante esta norma proporciona directrices para la gestión del riesgo en la seguridad de la información en una organización, dando soporte particular a los requisitos de un sistema de gestión de seguridad de la información (SGSI) de acuerdo con la norma ISO/IEC 27001. Sin embargo, esta norma no brinda ninguna metodología específica para la gestión del riesgo en la seguridad de la información. Se puede utilizar una variedad de metodologías existentes bajo la estructura descrita en esta norma para implementar los requisitos de un sistema de gestión de seguridad de la información [3].

Estructura ISO/IEC 27005:2009.

El proceso de gestión del riesgo en la seguridad de la información consta de:

- Establecimiento del contexto (numeral 7).
- Evaluación del riesgo (numeral 8).
- Tratamiento del riesgo (numeral 9).
- Aceptación del riesgo (numeral 10).
- Comunicación del riesgo (numeral 11).
- Monitoreo y revisión del riesgo (numeral 12).

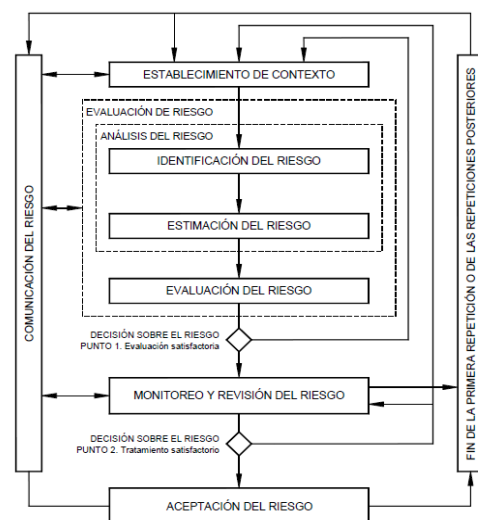


Fig. 4 Estructura ISO/IEC 27005, tomado de la norma ISO/IEC 27005:2009 [3]

Primero se establece el contexto, luego se realiza una valoración del riesgo, si ésta suministra la información suficiente para determinar de manera eficaz las acciones que se necesitan para mitigar los riesgos y lograr llevarlos a un nivel aceptable, entonces la labor está terminada y se continúa con el 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 para aceptar el riesgo o los criterios de impacto, posiblemente en partes limitadas del alcance total (véase la Figura 4, Decisión sobre el riesgo-punto 1).

La siguiente tabla resume las actividades de gestión del riesgo en la seguridad de la información alineadas con las cuatro fases del PHVA.

Proceso	Actividades de gestión del riesgo
Planificar	*Establecer el contexto *Valoración del riesgo (Identificación de Activos, Amenazas, Vulnerabilidades y Controles) *Planificación del tratamiento del riesgo *Aceptación del riesgo
Hacer	Implementación del plan de tratamiento del riesgo
Verificar	Monitoreo y revisión continuos de los riesgos
Actuar	Mantener y mejorar el proceso de gestión del riesgo en la seguridad de la información

Fig. 5 PHVA aplicado sobre las actividades de gestión del riesgo ISO/IEC 27005, tomado de la norma. ISO/IEC 27005:2009

La mayoría de las metodologías de riesgo se sustentan en la identificación de amenazas y vulnerabilidades entorno a los activos de información, sus respectivos controles para reducir el riesgo a niveles aceptables. Sin embargo cuando nos enfrentamos a un análisis de riesgo la primera pregunta que se debe plantear es ¿cómo se deben gestionar los riesgos?, ¿Cómo se debe realizar el análisis del riesgo? y ¿Cuál es la mejor forma de plantear el análisis de riesgos?, para determinar cuáles son las amenazas a las que está expuesta la información debido las vulnerabilidades propias de los activos de información; todo esto para dimensionar el nivel de riesgo al que se encuentra expuesta la organización.

V. ISO/IEC 20008:2008 – GESTIÓN DE LA SEGURIDAD EN LA CADENA DE SUMINISTRO

Esta es una norma de gestión de alto nivel que posibilita a una organización establecer un sistema de

gestión de la seguridad de la cadena de suministro en general. Exige a la organización evaluar el ambiente de seguridad en el que opera y determinar si se han implementado medidas de seguridad adecuadas y si ya existen otros requisitos de reglamentación que la organización cumple. Esta norma se basa en la metodología conocida como Planificar-Hacer-Verificar-Actuar (PHVA). Planificar: Establecer los objetivos y procesos necesarios para entregar resultados de acuerdo con la política de seguridad de la organización.

- Hacer: Implementar los procesos.
- Verificar: Supervisar y medir procesos contra la política de seguridad, objetivos, metas, requisitos legales y otros y reportar resultados.
- Actuar: Tomar acciones para mejorar continuamente el desempeño del sistema de gestión de la seguridad.

Estructura ISO/IEC 28000:2008 [6].

- Establecer los objetivos y las metas para la gestión de la seguridad.
- Establecer los programas de gestión de la seguridad.
- La determinación de los requisitos para el diseño, la especificación y la implantación.
- La identificación de los recursos necesarios.
- La identificación de las necesidades de formación y las habilidades.
- El desarrollo de los controles operacionales.
- El marco de trabajo para la gestión de los riesgos globales de la organización.

Teniendo en cuenta las metodologías expuestas se puede evidenciar que utilizando cualquiera de las dos metodologías “Margerit” o “ISO/IEC 27005:2009” se debe generar un inventario de activos de información, lo que puede convertirse en un problema, debido a que en tanto la organización sea pequeña este inventario será fácilmente manejable para gestionar los riesgos, pero cuando hablamos de una organización donde el promedio de procesos es mayor o igual a 20, y el promedio de los activos de información por proceso oscila entre 20 y 30 activos, surgen problemas como el tiempo requerido para la realización del inventario, adicionalmente realizar el análisis de riesgo sobre un inventario de activos muy extenso genera duplicidad de las amenazas y controles lo que conlleva al reprocesamiento de actividades, impactando de forma directa el rendimiento y la eficacia del análisis de riesgo.

Por otra parte ISO “31000:2009” no habla específicamente de activos de información, se centra en los procesos y hace énfasis en determinar el contexto de la organización tanto interno como externo fase en la que coincide con ISO/IEC 27005:2009.

Como se planteó anteriormente en los dos casos “Procesos vs Activos” existen ventajas y desventajas, sin embargo existen normas que ofrecen metodologías interesantes como la mencionada ISO/IEC 28000: 2008 en el numeral V, que se enfoca en la especificación los sistemas de gestión de seguridad para la cadena de suministro a través de la simplificación estratégica de las actividades en busca del mismo objetivo, realizar un análisis de riesgo efectivo en el menor tiempo posible. Esta norma plantea la definición de escenarios de riesgo, ¿qué es un escenario?, un escenario es un conjunto determinado de amenazas relacionado con un conjunto determinado de activos en el que se realiza una identificación de amenazas, controles e impactos sobre los escenarios y no sobre los activos de forma individual. Se evalúan grupos de activos contra grupos de amenazas. Esta metodología brinda ciertos beneficios como evitar la elaboración de un inventario demasiado detallado que en ocasiones genera costos elevados y gran complejidad en su actualización.

VI. METODOLOGÍA PARA LA GESTIÓN DE RIESGOS POR ESCENARIOS.

La metodología trabaja por escenarios de riesgo, simplificando el inventario de activos de información y optimizando su uso pero sin eliminarlo; teniendo en cuenta que esto facilita el análisis de vulnerabilidades y amenazas asociadas a los diferentes activos, los cuales a su vez se encuentran agrupados por escenarios de riesgo, evitando así duplicar las actividades de identificación de amenazas, vulnerabilidades y controles de remediación. Se debe tener especial cuidado a la hora de definir los escenarios de riesgo, debido a que de esta depende que se identifiquen todas las amenazas y vulnerabilidades pertinentes a la totalidad de los activos que conforman el escenario de riesgo, logrando así realizar un análisis de riesgo de forma efectiva y lo más acertada posible optimizando tiempo y recursos.

El análisis por escenarios interactúa también con los procesos permitiendo obtener una visión global de la organización y los riesgos potenciales a los que está expuesta, generando conciencia para obtener el apoyo requerido por parte de la alta gerencia.

La metodología propuesta toma como base los estándares ISO/IEC 27005:2011, ISO/IEC 31000:2011 e ISO/IEC 28000:2008; haciendo una fusión de los tres estándares, tomando las mejores prácticas de cada uno. La metodología se fundamenta en las siguientes fases:

1. Alineación de los estándares

La metodología busca fusionar la estructuras de las normas ISO/IEC 27005: 2009, ISO/IEC 31000:2011 e ISO/IEC 28000:2008 bajo el ciclo PHVA, complementándolas de forma estratégica como se muestra en la figura 6.

ISO/IEC 31000:2011	ISO/IEC 27005:2009	ISO/IEC 28000:2008
Mandato y compromiso de la alta gerencia		
Diseño del marco de referencia para la gestión del riesgo	Definición del plan de gestión de riesgos	Establecer los objetivos y las metas para la gestión de la seguridad
Entender la organización y su contexto	Establecer el contexto de la organización	La determinación de los requisitos para el diseño, la especificación y la implementación
Definición de responsabilidades		
Asignación de recursos		
Integración de procesos		
Establecer mecanismos de comunicación		
Valoración del riesgo	Identificación del riesgo	Gestión global de los riesgos a través de escenarios de riesgo
Estimación del riesgo	Evaluación del riesgo	Estimación del riesgo
Desarrollo del plan para el tratamiento de riesgos	Desarrollo del plan para el tratamiento de riesgos	Evaluación del riesgo
Políticas para la gestión del riesgo	Implementación del plan de tratamiento de riesgos	Desarrollo de controles operacionales
Implementación del marco de referencia para la gestión del riesgo		La identificación de las necesidades de formación y las habilidades
Implementación del proceso de gestión del riesgo	Implementar el plan de comunicación de riesgos	
Monitoreo y revisión	Monitoreo y revisión del riesgo	
Mejora continua	Mantener y mejorar el proceso de gestión	

Fig. 6 Alineación de estándares ISO/IEC 31000, ISO/IEC 27005 e ISO/IEC 2800 bajo el modelo PHVA, por el autor.

2. Pasos de la metodología

a. Definición de los escenarios:

En la definición del escenario de riesgo se debe tener en cuenta el nivel de afectación que tendrá cada uno de los escenarios sobre las propiedades de la seguridad de la información, “Confidencialidad”, “Integridad” y “Disponibilidad”. A continuación se relacionan los principales escenarios de riesgo.

- Información electrónica/digital
- Hardware
- Software/Aplicaciones
- Sitios WEB
- Servicios
- Infraestructura (Locaciones)
- Servidores IT
- Dispositivos (comunicaciones y seguridad)
- Base de Datos
- Personal

- Establecimiento del contexto.
- Establecimiento del plan de comunicación interno y externo.
- Valoración de riesgos por escenarios.
- Tratamiento de riesgos por escenarios.

- f. Monitoreo y mejora continua del proceso de gestión.

VII. CONCLUSIONES.

- La propuesta de integración de metodologías de riesgo plantea una estrategia para optimizar el tiempo y los recursos utilizados para la ejecución del análisis de riesgo.
- La metodología propuesta permite entender mejor los conceptos definidos en los estándares de gestión del riesgo citados.
- La gestión de riesgos es un factor fundamental para la implementación de seguridad de la información, debido a que permiten desarrollar estrategias para la mitigación de riesgos y ayudan crear conciencia en seguridad de la información para prevenir riesgos y obtener el apoyo de la alta gerencia con el fin de cumplir los objetivos de la seguridad de la información.
- La metodología para la gestión de riesgos por escenarios enfoca los procesos, activos, amenazas y vulnerabilidades en un análisis de riesgo efectivo que optimiza el tiempo de ejecución y el aprovechamiento de recursos, evitando el reprocesamiento de actividades debido a la duplicidad de amenazas y controles; de igual forma permitirá plantear planes de remediación globales frente a escenarios de riesgo.
- Las organizaciones deben fortalecer su protección en todos los escenarios de riesgo, a nivel físico (infraestructura locativa y tecnológica), a nivel lógico (software y sistemas de información) y el factor humano (en cuanto a medidas organizacionales y entrenamiento).
- La metodología integrada de riesgos por escenario se define como línea base para impartir lineamientos sobre cómo gestionar este tipo de riesgos a través de la agrupación de los activos, amenazas y vulnerabilidades por escenarios de riesgo, buscando la construcción de un marco de protección integral.

REFERENCIAS

- [1] PAe Portal administración electrónica, Metodología MARGERIT. Online disponible en: http://administracionelectronica.gob.es/ctt/magerit#.VWKHxPI_Oko
- [2] ISO (International Standard Organization). (2011). *Gestión del riesgo – Principios directrices. Estándar de Seguridad ISO 31000*.
- [3] ISO (International Standard Organization). (2009). *Tecnología de la información – Técnicas de seguridad – Gestión del riesgo de seguridad de la información. Estándar de Seguridad ISO/IEC27005*.
- [4] INTECO Instituto Nacional de Tecnologías de la Comunicación/ Enrique Bilbao Lázaro, www.cuevavaliente.com
- [5] *Gestión de riesgo - Seguridad Informática*
<https://seguinfo.wordpress.com/2013/07/01/iso-31000:2011-gestion-de-riesgos/>
- [6] ISO (International Standard Organization). (2008). *Sistemas de Gestión de la Seguridad para la cadena de suministro. Estándar ISO-IEC 28000*.

Ricardo Adolfo Velasco Cortes

Ingeniero de Sistemas Universidad INCCA de Colombia.
Aspirante a Especialista en Seguridad Informática
Universidad Piloto de Colombia.

Oficial de Seguridad de la Información en Datacenter
Colombia S.A.S.