Metodologías Para el Análisis de Riesgos en los SGSi

Methodologies for Analysis of Risks in the ISMS

[1]Helena Alemán Novoa, [2]Claudia Rodríguez Barrera

Fundación Universitaria Juan de Castellanos, Facultad de Ingeniería, Tunja, Boyacá, Colombia

[1]haleman@jdc.edu.co [2]crodriguez@jdc.edu.co

Recibido: 16/05/2014 • Aprobado: 22/06/2014

Resumen

Preservar la seguridad de los sistemas informáticos en la actualidad exige agotar una de las etapas más importantes que corresponde a la identificación, análisis y tratamiento de riesgos en toda la organización, dando a conocer oportunidades y amenazas que le permitan alcanzar sus objetivos de negocio y realizar una gestión proactiva. En este artículo se presenta una descripción general de las metodologías más relevantes de análisis de riesgos, Octave, Magerit, Mehari, NIST SP 800:30, Coras, Cramm y Ebios, aplicadas en el ámbito de la seguridad informática, lo que permitirá contextualizar y concientizar a las organizaciones en la necesidad de aplicarlas para la implementación de mecanismos de seguridad de acuerdo con los riesgos y amenazas identificados y, a su vez, integrar esta etapa dentro de los Sistemas de Gestión de Seguridad Informática SGSI con base en las normas y estándares existentes.

Palabras clave: *análisis de riesgos, gestión de riesgos, metodologías, seguridad, vulnerabilidad, SGSI.*

Abstract

To preserve the security of computer systems at present, demands to exhaust one of the most important stages corresponding to the identification, analysis and treatment of risks throughout the organization, publicizing opportunities and threats that enable it to achieve its business objectives and perform proactive management. This article presents an overview of the methodologies that are more relevant to risk analysis, Octave, Magerit, Mehari, NIST SP 800:30, Coras, Cramm and Ebios, applied in the field of computer security, which will contextualize and raise awareness of the organizations on the need to apply them for the implementation of security mechanisms in accordance with the risks and threats identified and, in turn, integrate this stage within the systems for the Management of Computer Security ISMS, according to existing rules and standards.

Keywords: *ISMS, methodologies, risk analysis, risk management, security, vulnerability.*

I. Introducción

La implementación de un Sistema de Gestión de Seguridad Informática (SGSI) se encuentra determinada por la estructura organizacional de las instituciones, lo que abarca características como: tipo, tamaño, objetivos, servicios, procesos, personal y requerimientos de seguridad que establece la misma, para lo cual se apoya en estándares internacionales tales como ISO/IEC 27001, norma en la que se describen un conjunto de herramientas corporativas que permiten establecer un plan de acción para la solución de problemas de seguridad a nivel técnico, organizativo y legislativo en una empresa. Estos sistemas utilizan como requisitos, estrategias como el análisis, evaluación y gestión de riesgos dentro del ciclo PHVA (planear, hacer, verificar y actuar), específicamente lo relacionado con la fase de planear, lo que requiere la selección de una metodología sistemática que permita obtener una visión clara y priorizada de los riesgos a los que se enfrenta la organización, identificando los más relevantes y priorizando medidas por implantar para minimizar la probabilidad de materialización de dichos riesgos o el impacto, en caso de materializarse.

En el presente escrito se presentan algunas de las metodologías utilizadas para realizar el análisis de riesgos exigido por la norma ISO 27001 en el marco de la implementación de los SGSI, dentro de las cuales están: Octave, Magerit, Mehari, NIST SP 800:30, Coras, Cramm y Ebios. A su vez, se hace una breve descripción en cuanto a sus características, ventajas y desventajas, lo que permitirá conocer y proporcionar otras posibilidades para la aplicación de cualquiera de ellas en la actividad del análisis de riesgos, conforme a lo establecido por la norma ISO 31000 (estándar para la gestión de riesgos) dentro de los SGSI en las organizaciones.

II. Desarrollo de Contenido

A. Metodologías de análisis de riesgos

La norma ISO 31000:2009 establece un conjunto de principios que se deben satisfacer para que la gestión del riesgo sea eficaz; recomienda que las organizaciones desarrollen, implementen y mejoren de manera continuada un marco de trabajo cuyo objetivo sea integrar el proceso de gestión del riesgo en los procesos de gobierno, de estrategia y de planificación, de gestión y de elaboración de informes, así como en las políticas, los valores y en la cultura de toda la organización [1]. Esta norma puede ser utilizada por cualquier entidad pública o privada, organizaciones sin ánimo de lucro, asociaciones, grupos o individuos [2].

Los principios básicos de la gestión del riesgo que se describen en la norma ISO 31000 corresponden a: crear y proteger el valor, es una parte integral de todos los procesos de la organización, es parte de la toma de decisiones, trata explícitamente la incertidumbre, es sistémica, estructurada y oportuna, se basa en la mejor información disponible, es adaptable, integra los factores humanos y culturales, es transparente y participativa, es dinámica, iterativa, responde a los cambios y facilita la mejora continua de la organización [3].

Es así, como el análisis de riesgos informáticos pasa a ser una parte fundamental en la administración de la seguridad, permitiendo algunos beneficios, tal como, identificar los puntos más débiles de la estructura de TI que da soporte a los procesos críticos de la organización. Igualmente, además de ser una guía de selección de medidas de protección de costo adecuado, determina dónde es necesario contar con esquemas de recuperación de desastres y continuidad de negocio y permite realizar políticas de seguridad mejor adaptadas a las necesidades de la organización [4].

En el ámbito de la seguridad informática, las metodologías de análisis de riesgos conforman una disciplina que se articula desde los Sistemas de Gestión de Seguridad Informática SGSI en las organizaciones, realizando unos importantes escaneos de vulnerabilidades mediante el uso de una serie de modelos y procesos para, así, proponer una forma más segura de cuidar la información y los recursos de TI [5]. Algunos de los objetivos de las metodologías de análisis de riesgos corresponden a: planificación de la reducción de riesgos, prevención de accidentes, visualización y detección de las debilidades existentes en los sistemas y ayuda en la toma de las mejores decisiones en materia de seguridad de la información [6].

En la seguridad de la información existen diversas metodologías de análisis de riesgos dentro de las que sobresalen: Octave [7], Magerit [8], Mehari [9], NIST SP 800:30[10] y Coras [11], Cramm [43] y Ebios [47], las cuales se describen a continuación:

1) **Octave (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*).** Es una de las metodologías de análisis de riesgos más utilizada por las empresas. Esta describe un conjunto de criterios para desarrollar métodos que se adhieran a guías específicas de evaluación y administración de riesgos [4]. Octave evalúa los riesgos de seguridad de la información y propone un plan de mitigación de los mismos dentro de una organización. Sus objetivos se encuentran enfocados básicamente en concientizar a la organización en cuanto a que la seguridad informática no es un asunto solamente técnico, y presentar los estándares internacionales que guían la implementación de seguridad de aquellos aspectos no técnicos [12].

Este tipo de metodología realiza diversos procesos. Inicia con una evaluación de los activos relacionados con la información, para luego asignarles un valor estimado para la organización; de esta manera, la metodología Octave analiza y estudia la infraestructura de la información, definiendo así los elementos más importantes para la empresa [13]. Es una técnica de organización, proyección, clasificación y consultoría importante en seguridad de la información establecida en el riesgo; esta técnica logra su misión en tres procesos: auto dirigido, flexible y evolucionado, que a su vez, se desarrolla en tres fases: perfiles de amenazas basados en activos, identificación de vulnerabilidades de la infraestructura y desarrollo de estrategia y planes de seguridad [14].

La metodología Octave orienta a la organización para que dirija y gestione sus evaluaciones de riesgo, tome decisiones basadas en sus riesgos, proteja los activos críticos de información y comunique de forma efectiva la información clave de seguridad, para que, así, obtenga los siguientes beneficios: permitir la identificación de riesgos de la seguridad que puedan impedir la consecución del objetivo de la organización; enseñar a evaluar los riesgos de la seguridad de la información; crear una estrategia de protección con el objetivo de reducir los riesgos de seguridad de la información prioritaria y ayudar a la organización a cumplir regulaciones de la seguridad de la información [13].

En conclusión, Octave es un método operativo, orientado a resultados. Después de la primera iteración (2-3 meses) se obtiene un plan a corto plazo y un plan estratégico a largo plazo para mitigar los riesgos detectados. En la siguiente iteración (después de 6 meses o un año) se parte de los resultados de la implantación de las acciones anteriores; propone una metodología muy bien detallada, con unos pasos muy claros y definidos, proporcionando el suficiente material de soporte (plantillas, ejemplos, etc.) y asumiendo todas las buenas prácticas de las normas y estándares actuales [15].

2) Magerit. Es la metodología de análisis y gestión de riesgos de la información desarrollada por el Consejo Superior de Administración Electrónica. [16]. En la introducción de esta

metodología sobresalen dos objetivos principales, uno de los cuales es estudiar los riesgos que soporta un sistema de información y el entorno asociado a este, entendiendo por riesgo la posibilidad de que suceda un daño o perjuicio, en una primera aproximación que se atiene a la aceptación habitual del término, y otro relacionado con recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir impedir, reducir o controlar los riesgos investigados [17].

Siguiendo la terminología de la norma ISO 31000, *Estándar sobre principios y directrices para la gestión de riesgo* [18], Magerit responde a lo que se denomina "Proceso de Gestión de los Riesgos", sección 4.4 ("Implementación de la Gestión de los Riesgos") dentro del "Marco de Gestión de Riesgos"; es decir, Magerit implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información [19].

Magerit define la seguridad como "la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o mal intencionadas que comprometen la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles" [20].

Los principales elementos para el análisis de riesgos, según Magerit son: activo, amenaza, vulnerabilidades, impacto, riesgo y salvaguardas (funciones, servicios y mecanismos) [21].

De la misma manera, de acuerdo con Magerit, el proceso de análisis de riesgos se desarrolla en las siguientes etapas: planificación, análisis de riesgos, gestión de riesgos y selección de salvaguardas [22].

Magerit detalla la metodología desde tres perspectivas: describe los pasos para realizar un análisis del estado del riesgo y gestionar su mitigación; describe las tareas básicas para realizar un proyecto de análisis y gestión de riesgos y uno de sus capítulos aplica la metodología al caso del desarrollo de Sistemas de Información (SI). Adicionalmente, muestra una serie de aspectos prácticos derivados de la experiencia acumulada en el tiempo para el análisis y gestión del riesgo de manera efectiva [23].

Esta metodología ayuda a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control y apoyar en la preparación de la organización para procesos de evaluación, auditoría, certificación o acreditación; así mismo, una de sus mayores ventajas es que las decisiones que deban tomarse y que tengan que ser validadas por la dirección estarán fundamentadas y serán fácilmente defendibles. Otro de sus aspectos positivos radica en que sus resultados se expresan en valores económicos lo que, a su vez, también es una desventaja por cuanto el hecho de tener que traducir de forma directa todas las valoraciones en valores económicos, hace que la aplicación de esta metodología sea muy costosa [24].

***3) Mehari*.** Método Armonizado de Análisis de Riesgos. Esta metodología fue propuesta y desarrollada por el Club Francés de la Seguridad de la Información CLUSIF en el año 1996; es de acceso público y para todo tipo de organizaciones. Se diseñó inicialmente y se actualiza continuamente para ayudar a los CISO (*Chief Information Security Officers*) en la gestión de las actividades de la seguridad informática, pero también está concebida para auditores CIO o gestores de riesgos [25]. Es una metodología utilizada para apoyar a los responsables de la seguridad informática de una empresa mediante un análisis riguroso de los principales factores de riesgo, evaluando cuantitativamente, de acuerdo con la situación de la organización, dónde se requiere el análisis; acopla los

objetivos estratégicos existentes con los nuevos métodos de funcionamiento de la empresa mediante una política de seguridad y mantenimiento de los riesgos a un nivel convenido. Mehari propone un módulo para analizar los intereses implicados por la seguridad y un método de análisis de riesgos con herramientas de apoyo [26].

El principal objetivo de Mehari es proporcionar un método para la evaluación y gestión de riesgos, concretamente en el dominio de la seguridad de la información, conforme a los requerimientos ISO/IEC 27005:2008, por medio de un conjunto de herramientas y elementos necesarios para su implementación [27] [28].

Los aspectos fundamentales de esta metodología son: diseño de un modelo de riesgo, evaluación de la eficiencia de las políticas de seguridad previamente planteadas en la organización y capacidad para valorar y simular los niveles de riesgo. Sus archivos e instrumentos oficiales hacen énfasis en un marco metodológico y una base de conocimientos con la finalidad de investigar y realizar un análisis de los diferentes inconvenientes y falencias que se presentan, poner en consideración las vulnerabilidades en los sistemas de información, dar solución a las mismas, disminuir y controlar los riesgos y supervisar la seguridad de la información [29]. Con Mehari se detectan vulnerabilidades mediante auditorías, se analizan situaciones de riesgo y se razonan sus contextos [30].

Esta metodología puede ser utilizada con un método continuo de trabajo o como soporte a otras experiencias de la gestión de la seguridad de la información [31].

Mehari es ante todo un procedimiento de sistemas de auditoría y evaluación de riesgos; la gestión se diseñó y programó para un análisis profundo y verídico de los riesgos en sistemas informáticos. Cuenta con tres módulos: análisis o evaluación de riesgos, evaluación de seguridad (centrada en el análisis de vulnerabilidades) y análisis de amenazas [32], los cuales pueden ser seleccionados con base en las políticas y estrategias corporativas a fin de decidir y construir planes de acción encaminados a mantener la seguridad de la información.

4) NIST SP 800 – 30. (*National Institute of Standards and Technology*): *Guía de gestión de riesgo para sistemas de tecnología de la información – Recomendaciones del Instituto Nacional de Estándares y Tecnología* [33]. Es una guía que propone un conjunto de recomendaciones y actividades para una adecuada gestión de riesgos como parte de la gestión de la seguridad de la información; sin embargo, esto no es suficiente, pues se necesita del apoyo de toda la organización para que los objetivos y alcance de la gestión de riesgos concluyan con éxito [34]. La Metodología NIST SP 800-30 está compuesta por 9 pasos básicos para el análisis de riesgo:

- Caracterización del sistema.
- Identificación de amenaza.
- Identificación de vulnerabilidades.
- Control de análisis.
- Determinación del riesgo.
- Análisis de impacto.
- Determinación del riesgo.
- Recomendaciones de control [35].

Esta metodología proporciona una base para development of an effective risk management program, containing both the definitions and theel desarrollo de un programa eficaz de gestión de riesgos que contiene las definiciones y la practical guidance necessary for assessing and mitigating risks identified within IT systems. orientación práctica necesaria para evaluar y mitigar los riesgos identificados dentro de los sistemas de TI. Su objetivo final es ayudar a las organizaciones a gestionar mejor los riesgos mediante un proceso de tres pasos: evaluación, mitigación, análisis y evaluación del riesgo [36]. NIST se destaca por la gestión de riesgos en proyectos de TI y alcanza niveles satisfactorios en hardware, software, BD,

redes y telecomunicaciones, pues en su estructura se establecen criterios de seguridad, siendo los más comunes, la confidencialidad, integridad y disponibilidad, los cuales son la base para realizar el análisis y valorar la materialización de amenazas e impactos sobre los elementos de TI [37]. No obstante, al ser una metodología tan robusta, esta propiedad se convierte en una limitante para su aplicación en pequeñas empresas con altas limitaciones de recursos humanos [38].

5)* Coras – *Construct a Platform for Risk Analysis of Security Critical Systems. *Consultative Objetive Risk Analysis System* es un proyecto desarrollado desde el año 2001 por Sintef, un grupo de investigadores noruego financiado por organizaciones del sector público y privado [39], cuya misión es proporcionar un marco de trabajo encaminado a sistemas en los que la seguridad es crítica. Su aplicación permite la detección de fallas de seguridad, inconsistencias, redundancia y el descubrimiento de vulnerabilidades de seguridad, exploradas en siete etapas: presentación, análisis de alto nivel, aprobación, identificación de riesgos, estimación de riesgo, evaluación de riesgo y tratamiento del riesgo [40].

Se trata de una técnica que es muy útil para equipos heterogéneos que intenten identificar vulnerabilidades y amenazas a sus activos de valor [41]. Esta metodología suministra un método basado en modelos, acompañado específicamente de los siguientes componentes:

- Una metodología de análisis de riesgos basado en la elaboración de modelos.
- Un lenguaje gráfico basado en UML (*Unified Modelling Language*).
- Un editor gráfico para soportar la elaboración de modelos (*Microsoft Visio*).
- Una biblioteca de casos reutilizables.
- Una herramienta de gestión de casos (gestión y reutilización de casos).
- Representación textual basada en XML (*eXtensible Mark-up Language*).
- Un formato estándar de informe para facilitar la comunicación de distintas partes en el proceso de análisis de riesgos. [40].

EL método Coras provee un editor gráfico en el cual se diseñan los modelos de lenguaje basados en *Microsoft Visio*, una librería de casos reutilizables, un objeto de gestión de casos y un formato general de informes, el cual facilita la comunicación entre diferentes partes del proceso de análisis de riesgo [42].

***6)* Cramm (CCTA *Risk Analysis and Management Method*).** Es una metodología de análisis de riesgos, desarrollada por el *Central Communication and Telecommunication Agency* (CCTA) del gobierno del Reino Unido, utilizada, por lo general, en Europa [43] y dirigida a grandes industrias, entre otras, organizaciones gubernamentales. Así mismo, Cramm se divide en tres etapas: en la primera se establecen los objetivos de seguridad; en la segunda se hace el análisis de riesgos y en la tercera, la identificación y selección de salvaguardas [44]. Cramm puede definirse como una Metodología para el análisis y gestión de riesgos encaminada a brindar confidencialidad, integridad y disponibilidad de los sistemas de información mediante el uso de una evaluación mixta. [45] La OTAN, el Ejército de Holanda y numerosas organizaciones de todo el mundo la utilizan actualmente [46].

7) Ebios - Expresión de las necesidades e identificación de los objetivos de seguridad [47]. Es una metodología francesa de análisis y gestión de riesgos de seguridad de sistemas de información que comprende un conjunto de guías y herramientas de código libre, enfocada a gestores del riesgo de TI [48]. Esta metodología se

desarrolla mediante cinco (5) fases: Fase 1: estudio del contexto; Fase 2: estudio de los eventos peligrosos; Fase 3: estudio de los escenarios de amenazas; Fase 4: estudio de los riesgos; Fase 5: estudio de las medidas de seguridad, Caso práctico [49]. Es una herramienta completa que permite evaluar y abordar los riesgos relacionados con la seguridad informática promoviendo una eficaz comunicación dentro de la organización y entre sus socios, dando cumpliendo a los últimos estándares de la ISO 27001, 27005 y 31000 [50] para la gestión de riesgos y brindando las justificaciones necesarias para la toma de decisiones (descripciones precisas, retos estratégicos, riesgos detallados con su impacto en el organismo, objetivos y requerimientos de seguridad explícitos). Ebios es una verdadera herramienta de negociación y arbitraje [51].

B. Aplicación de las metodologías de análisis de riesgos

Una vez revisadas las diferentes metodologías, se han aplicado en algunos casos específicos, como el de la Fundación Universitaria Juan de Castellanos, siendo referente para la implementación de un SGSI basado en la norma ISO 27001, dentro de la cual se exige realizar el análisis de riesgos, lo que ha permitido contrastar algunas ventajas y desventajas que se describen en la Tabla No. 1.

TABLA I.

Ventajas y Desventajas de las Metodologías de Análisis de Riesgos

METODOLOGÍA	ÁMBITO DE APLICACIÓN	VENTAJAS	DESVENTAJAS
OCTAVE	Pymes, organizaciones públicas y privadas.	Es autodirigible. Se puede desarrollar por empleados de la misma organización, utilizando un equipo multidisciplinario. Involucra a todo el personal. Construcción de los perfiles de amenazas basados en activos. Identificación de la infraestructura de vulnerabilidades. Desarrollo de planes y estrategias de seguridad. Comprende las etapas de análisis y gestión de riesgos. Involucra procesos, activos, dependencias, recursos, vulnerabilidades, amenazas y salvaguardas. Relaciona amenazas y vulnerabilidades. Uso interno: gratuito. Posee tres métodos Octave, Octave-s y Octave allegro, adaptables a una organización.	No tiene en cuenta el principio de no repudio de la información. Utiliza muchos documentos en el proceso de análisis de riesgos. Se requiere de amplios conocimientos técnicos. No define claramente los activos de información. Uso externo: se debe comprar la licencia al SEI si se quiere implementar la metodología a un tercero.

METODOLOGÍA	ÁMBITO DE APLICACIÓN	VENTAJAS	DESVENTAJAS
MAGERIT	Gobierno, compañías grandes comerciales y no comerciales, Pymes.	Alcance completo en el análisis y gestión de riesgos. Está bien documentada en cuanto a recursos de información, amenazas y tipos de activos. Utiliza un completo análisis de riesgo cuantitativo y cualitativo. Es libre y no requiere autorización para su uso. Divide los activos de la organización en diferentes grupos, para identificar más riesgos y poder tomar contramedidas para evitar así cualquier riesgo. Se centra en tres objetivos: concientizar sobre la existencia de los riesgos y de la necesidad de atajarlos a tiempo, ofrecer un método sistemático para analizar tales riesgos, ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control. Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación. Permite que el proceso esté bajo control en todo momento y contempla aspectos prácticos para la realización de un análisis y una gestión de riegos efectiva. Posee una buena base documental en tres libros: El método, Catálogo de elementos y Guía de técnicas, que son de acceso público. Posee herramientas para el análisis de riesgo como PILAR.	En su modelo no involucra los procesos, recursos, ni vulnerabilidades. Posee falencias en el inventario de políticas. Se considera una metodología costosa en su aplicación.
MEHARI	Gobierno, organismos, empresas grandes y medianas, compañías comerciales sin ánimo de lucro (educación, salud, servicios públicos, organizaciones privadas).	Para su análisis de riesgos utiliza un modelo cuantitativo y cualitativo. Es un método capaz de evaluar y lograr la disminución de riesgos en función del tipo de organización. Posee bases de datos de conocimientos con manuales, guías y herramientas que permiten realizar el análisis de riesgos cuando sea necesario. Complementa y se acopla a las necesidades de la norma ISO 27001, 27002 y 27005 para definir los SGSI y la gestión de riesgos. Por medio de esta metodología se detectan vulnerabilidades mediante auditorías y se analizan las situaciones de riesgo. Combina análisis y evaluación de riesgos; particularmente, se especifica un módulo de evaluación rápida y uno de evaluación detallada.	Se enfoca solo en los principios de integridad, confidencialidad y disponibilidad, olvidando el no repudio. La recomendación de los controles no se incluye dentro del análisis sino dentro de la gestión de los riesgos. El impacto de los riesgos se estima en el proceso de gestión y evaluación.

METODOLOGÍA	ÁMBITO DE APLICACIÓN	VENTAJAS	DESVENTAJAS
NIST SP 800 - 30	Utilizada por organizaciones gubernamentales y no gubernamentales.	Bajo costo relacionado con el riesgo analizado y solventado. Proporciona una guía para evaluación de riesgos de seguridad en las infraestructuras de TI. Presenta un resumen de los elementos clave de las pruebas de seguridad técnica y la evaluación con énfasis en técnicas específicas, sus beneficios, limitaciones y recomendaciones para su uso. La guía provee herramientas para la valoración y mitigación de riesgos. Asegura los sistemas informáticos que almacenan, procesan y transmiten información. Mejora la administración a partir de los resultados del análisis de riesgos. Se aplica en el análisis y la gestión de los riesgos.	En su modelo no tiene contemplados elementos como los procesos, los activos ni las dependencias.
CORAS		Posee diferentes herramientas de apoyo para el análisis de riesgos, un editor gráfico para soportar la elaboración de los modelos basado en Microsoft Visio y utiliza lenguaje grafico basado en UML (Unified Modelling Language). Provee un repositorio de paquetes de experiencias reutilizables. Provee un reporte de las vulnerabilidades encontradas. Útil en el desarrollo y mantenimiento de nuevos sistemas. Basada en modelos de riesgos de sistemas de seguridad críticos.	No realiza análisis de riesgos cuantitativo. En su modelo no tiene contemplados elementos como los procesos y las dependencias.

METODOLOGÍA	ÁMBITO DE APLICACIÓN	VENTAJAS	DESVENTAJAS
CRAMM	Organizaciones públicas y privadas.	Aplica los conceptos de manera formal, estructurada y disciplinada protegiendo los principios de seguridad y sus activos. Realiza un análisis de riesgos cualitativo y cuantitativo. Es aplicable a todo tipo de sistemas y redes de información y se puede utilizar en todas las etapas del ciclo de vida del sistema de información desde la planificación y viabilidad, por medio del desarrollo e implementación del mismo. Se puede usar siempre que sea necesario para identificar la seguridad y/o requisitos de contingencia para un sistema de información o de la red. Identifica y clasifica los activos de TI. Evalúa el impacto empresarial. Identifica y evalúa amenazas y vulnerabilidades, evalúa niveles de riesgo e identifica los controles requeridos. Compuesta por más de 4.000 contramedidas reunidas en grupos y subgrupos con los mismos aspectos de seguridad, incluyendo activos de software, hardware y protecciones medioambientales. Combina análisis y evaluación de riesgos.	En su modelo no tiene contemplados elementos como los procesos y los recursos.
EBIOS	Es utilizada ampliamente en el sector público (en los Ministerios) y en el sector privado (pequeña y grandes empresas).	Ayuda a las organizaciones a tener un mayor reconocimiento en sus actividades de seguridad ya que esta tiene compatibilidad con las normas internacionales como la ISO. Es una herramienta de negociación y de arbitraje. Es utilizada para múltiples finalidades y procedimientos de seguridad. Herramienta de código libre y reutilizable. Se acopla al cumplimiento de los estándares ISO 27001, 27005 y 31000. Herramienta de concienciación para involucrar a las partes involucradas (directivas, empleados, usuarios). Posee una base de conocimiento que describe tipos de entidades, métodos de ataque, vulnerabilidades, objetivos y requerimientos de seguridad.	Se constituye más como una herramienta de soporte.

III. Conclusiones

Es importante establecer una metodología de análisis de riesgos dentro de los SGSI, lo que permitirá dar a conocer las debilidades y fortalezas con que cuenta una organización por cada uno de sus activos informáticos; se logrará identificar y valorar los procesos más críticos del negocio, con el propósito de evaluar el nivel de protección adecuado, determinar y evaluar las amenazas y su grado de efectividad para hacer frente a los riesgos y calcular el nivel de los mismos, de tal forma, que la organización conozca con detalle la probabilidad de materialización de cada una de las amenazas y el impacto que estas pueden ocasionar.

Cada una de las metodologías anteriormente expuestas ofrece un método sistematizado para identificar y analizar los riesgos, además de planificar las medidas necesarias para reducirlos y brindan herramientas que faciliten su análisis.

Las metodologías Octave, Magerit, Mehari, NIST SP 800, Coras, Cramm y Ebios poseen sus propias características y se complementan entre sí, lo que les permite, a su vez, combinar otros enfoques que hacen el proceso de análisis y gestión de los riesgos más robusto y eficiente.

Referencias

[1] C. Cerra, ISO 31000:2009. Herramienta para evaluar la gestión de riesgo, Uruguay. [On Line]. Disponible en: http://www.isaca.org/chapters8/Montevideo/cigras/Documents/cigras2011-cserra-presentacion1%20modo%20de%20compatibilidad.pdf.

[2] M. Castro, El Nuevo Estándar para la Gestión del Riesgo. [On Line]. Disponible en: http://www.surlatina.cl/contenidos/archivos_articulos/13-el%20nuevo%20estandar%20iso%20para%20la%20gestion%20del%20riesgo.pdf

[3] ISO 31000:2009-Setting a New Standard for Risk Management, Risk Analysis, Vol. 30, No. 6, 2010 [On Line]. Disponible en: http://esvc001356.wic015u.server-web.com/pdfs/articles/art_riskanalysis_iso31000.pdf

[4] E. Daltabuit, L. Hernández, J. Vázquez. La Seguridad de la Información, México: Limusa Noriega Editores S.A., 2009.

[5] M. Doris. Metodologías de la seguridad informática. [On line]. Disponible en: http://seguridadinformatica.bligoo.ec/media/users/22/1142179/files/312461/Metodologia_de_la_Seguridad_Ing.pdf

[6] J. Eterovic y G. Pagliari, Metodología de Análisis de Riesgos Informáticos. [Online]. Disponible en: http://www.cyta.com.ar/ta1001/v10n1a3.htm.

[7] E. José (2013, Septiembre), Octave, Metodología para el análisis de riesgos de TI, Periódico de los universitarios Universo, [On line]. Disponible en: http://www.uv.mx/universo/535/infgral/infgral_08.html

[8] G. Camilo (2013, Mayo) Magerit: metodología práctica para gestionar riesgos, welivesecurity en español [On line]. Disponible en: http://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

[9] Club de la securite de lìnformation francais, mehari, [On line]. Disponible en: https://www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Introduccion.pdf

[10] NIST, *information security, national Institute of Standards and Technology* [On line]. Disponible en: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

[11] Metodología Coras (*Construct a platform for Risk Analysis of Security critical system*) [On line]. Disponible en: http://seguridades7a.blogspot.com/p/coras.html

[12] A. Ana, Análisis de Riesgos en Seguridad de la Información, Ciencia Innovación y Tecnología, Facultad de Ingeniería. Fundación Universitaria Juan de Castellanos.

[13] P. Jose. Metodologías y normas para el análisis de riesgos. ISACA, [On line]. Disponible en: http://www.isaca.org/chapters7/Monterrey/Events/Documents/20100302%20Metodolog%C3%ADas%20de%20Riesgos%20TI.pdf

[14] R. Gómez, D. H. Pérez, Y. Donoso y A. Herrera. (2012, Enero) Metodología y gobierno de la gestión de riesgos de tecnologías de la información. [On line]. Disponible en: https://revistaing.uniandes.edu.co/pdf/A10%2031.pdf

[15] Atos Consulting, Metodología ISIS, Guía para el Diseño y Elaboración de Planes de Sistemas en Asociaciones de Mujeres. (2007, Abril). [On line]. Disponible en: http://www.celem.org/pdfs/GUIA_ISIS_DEF_acrobat.pdf

[16] Magerit v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, [On line]. Disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VRMl5_yG8ms

[17] M. Juan. Planes de Contingencia: La Continuidad del Negocio en las Organizaciones, España: Ediciones Díaz de Santos, 2006.

[18] Icontec, Norma Técnica Colombiana, NTC – ISO 31000, Gestión del Riesgo Principios y Directrices, Colombia: Edición Icontec, 2011.

[19] Magerit v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, [On line]. Disponible en: https://www.ccn-cert.cni.es/publico/herramientas/Pilar-5.4.1/web/magerit/Libro_I_metodo.pdf.

[20] B. David y R. Camilo. Modelo para la cuantificación del riesgo telemático en una organización, Venezuela: Red Enlace, 2010.

[21] Ministerio de Admisiones Públicas. Magerit Versión 2- Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, [On line]. Disponible en: http://www.defensa.gob.es/eu/Galerias/politica/infraestructura/sistemas-cis/DGN-CIS-metodo-v11-final.pdf

[22] Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Guía para responsables del dominio protegible [On line]. Disponible en: http://dis.um.es/~barzana/Curso03_04/MAGERIT.pdf

[23] Guía avanzada de gestión de riesgos, Inteco (2008, Diciembre), [On line]. Disponible en: https://www.incibe.es/file/TnOIvX7kM5r8OY-S8r9Bmg

[24] A. Carvajal, (2008). Análisis y Gestión del Riesgo, Base Fundamental del SGSI, Caso: Metodología Magerit [On line]. Disponible en: http://52.0.140.184/typo43/fileadmin/Base_de_Conocimiento/VIII_JornadaSeguridad/17-ElAnalisisRiesgosBaseSistemaGestionSeguridadInformacionCasoMagerit.pdf

[25] Club de la Sécurité de l'Information Français, Mehari, [On line]. Disponible en: http://www.clusif.asso.fr/en/clusif/present/

[26] M. Gallardo, P. Jácome (2011, Febrero). Análisis de Riesgos Informáticos y Elaboración de un Plan de Contingencia T.I. para la Empresa eléctrica Quito S.A. [On line]. Disponible en: http://bibdigital.epn.edu.ec/bitstream/15000/3790/1/CD-3510.pdf

[27] M. Crespo. (2014), El Análisis de Riesgos dentro de un Auditoría Informática: Pasos y Posibles Metodologías, [On line]. Disponible en: http://hinaluz.blogspot.com/

[28] Seguridad informática, objetivos de las metodologías de análisis de riesgos, (2014, Marzo) [On line]. Disponible en: http://seguridadinformaticaunad.blogspot.com/2014/03/metodologias-de-evaluacion-del-riesgo.html

[29] G. Luz. (2014, Marzo), Metodologías Riesgo y Control Informático, [On line]. Disponible en: http://hinaluz.blogspot.com/

[30] J. Poveda, (2011, Marzo). Análisis y valoración de los Riesgos Metodologías On line]. Disponible en: https://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-8.pdf

[31] C. Camilo. Metodología para el Análisis de Riesgos, (2014, diciembre) [On line]. Disponible en: http://camilo-cruz-ucatolica-riesgos.blogspot.com/2014/12/mehari.html

[32] M. Crespo, (2013), El Análisis de Riesgos dentro de una Auditoría Informática: Pasos y posibles metodologías [On line]. Disponible en: http://e-archivo.uc3m.es/bitstream/handle/10016/16802/PFC_Carmen_Crespo_Rin.pdf?sequence=1

[33] R. Alexandra, O. Zulima. (2011), Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios, *Ingeniería* 16(2), 56-66.

[34] V. Avalos, "Desarrollo de una aplicación para la gestión de riesgos en los sistemas de información utilizando la guía metodológica NIST SP 800-30 caso práctico Liceo Del Valle", Tesis, Escuela Politécnica del Ejército, [On line]. Disponible en: http://repositorio.espe.edu.ec/handle/21000/2333

[35] Seguridad 7"A"Metodología NIST SP 800-30 *(National Institute of Standards and Technology*), [On line]. Disponible en: http://seguridades7a.blogspot.com/p/nist-sp-800-30.html.

[36] Comisión interamericana de Telecomunicaciones, gestión de riesgos de seguridad (2009), [On line]. Disponible en: http://www.oas.org/en/citel/infocitel/2009/septiembre/seguridad_e.asp

[37] C. Jonathan. Gestión del riesgo en las metodologías de proyectos de tecnologías de información y comunicaciones (2013).

[38] M. Luis y G. Diego. Validación de un método ágil para el análisis de riesgos de la información digital, [On line]. Disponible en: http://investigaciones.usbcali.edu.co/ockham/images/volumenes/Volumen9N2/vol9n2_07.pdf

[39] Análisis y Modelado de Amenazas, metal.hacktimes.com (2006) [On line]. Disponible en: https://fortinux.com/wp-content/uploads/2010/12/Analisis-y-Modelado-de-Amenazas.pdf

[40] M. Juan. (2009), Análisis de Riesgos de Seguridad, [On line]. Disponible en: http://oa.upm.es/1646/1/PFC_JUAN_MANUEL_MATALOBOS_VEIGAa.pdf

[41] Análisis de amenazas en ataques dirigidos tipo APT: caso práctico con el método Coras Security Advisors,(2014), [On line]. Disponible en: https://ssa-asesores.es/wordpress/blog/2014/06/02/analisis-de-amenazas-en-ataques-dirigidos-tipo-apt-caso-practico-con-el-metodo-coras/

[42] C. Elvis, Metodología para el análisis de riesgos en seguridad informática,), [On line]. Disponible en: http://msnseguridad.blogspot.com/2012/08/seguridad-informatica-la-seguridad.html

[43] Seguridad en Redes de Telecomunicaciones e Informática, CRAMM: Software para el manejo de Riesgos (2010, Julio) [On line]. Disponible en: http://seguridaddigitalvenezuela.blogspot.com/2010/07/cramm-software-para-el-manejo-de.htm

[44] Documento de Seguridad y defensa 60. Estrategia de la información y seguridad en el ciberespacio, Centro Superior de Estudios de la Defensa Nacional y Escuela de Altos Estudios de la defensa. Editorial Ministerio de defensa (2014) [On line]. Disponible en: http://www.uma.es/foroparalapazenelmediterraneo/wpcontent/uploads/2014/07/dsegd_60.pdf

[45] C. Leonardo. Seguridad de la Información en Colombia (2010, Mayo) [On line]. Disponible en http://seguridadinformacioncolombia.blogspot.com/2010/05/gestion-de-riesgos.html

[46] UNFV- Seguridad & auditoría, metodología para identificar la amenaza de los activos (II), (2011, Junio) [On line]. Disponible en: http://villarrealino-seguridad-yauditoria.blogspot.com/2011/06/metodologia-para-identificar-la-amenaza.html

[47] D. Márquez y A.V. Marcano. Modelo de Estrategias Integrales de Seguridad Para La Infraestructura de Red De Datos. Caso de Estudio: Universidad de Oriente Núcleo Monagas. Panamá. [On line] Disponible en: http://www.laccei.org/LACCEI2012-Panama/RefereedPapers/RP099.pdf

[48] Tangient LLC. (2014). EBIOS - Metodología Francesa Análisis y Gestión de Riesgos. Retrieved marzo 21, 2014, from EBIOS - Metodología Francesa Análisis y Gestión de Riesgos: [On line]. Disponible en: http://seguridadinformaticaufps.wikispaces.com/EBIOS+y-+Metodologia+Francesa+Analisis+y+Gesti%C3%B3n+de+Riesgos

[49] Ebios Advanced Practioner, Metodología EBIOS, 2015 [On line]. Disponible en: https://www.phosforea.com/main/es/pdf/05/ebios_advanced_practitioner.pdf

[50] ANSSI, la méthode EBIOS. [On line]. Disponible en: http://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/.

[51] Republique Francaise, Premier Ministre, Secrétariat général de la défense nationale, El método EBIOS, [On line]. Disponible en: http://www.ssi.gouv.fr/archive/es/confianza/documents/methods/ebiosv2-methode-plaquette-2003-09-01_es.pdf