UNIVERSIDAD DEL AZUAY

UDA AKADEM

Facultad de Ciencias de la Administración

Número

1

ESTUDIO COMPARATIVO ENTRE LAS METODOLOGÍAS CRAMM Y MAGERIT PARA LA GESTIÓN DE RIESGO DE *TI* EN LAS MPYMES

Esteban Crespo Martínez
Geovanna Cordero Torres

Resumen

Lograr el objetivo de proponer una metodología de seguridad de la información para la gestión del riesgo informático, aplicable al entorno empresarial y organizacional, del sector MPYME ecuatoriano, requiere del análisis de las metodologías Magerit y CRAMM (CCTA Risk Analysis and Management Method), las mismas que son internacionalmente utilizadas en la gestión del riesgo de información; contemplando los marcos de referencia que contienen las mejores prácticas de la industria: ISO 27001, 27002, 27005 y 31000.

Palabras clave: riesgos, gestión, Magerit, CRAMM, tecnologías de información, TI, seguridad, información, SGSI.

Abstract

This paper aims to study the CRAMM (CCTA Risk Analysis and Management Method) and Magerit methodologies used in information risk management. It contemplates international reference frames that contain the best practices in the industry: ISO 27001, 27002, 27005 and 31000. This research is part of a project proposal of “Methodology for information security risk management, applicable to MSMEs” applicable to the Ecuadorian environment.

Keywords: Risk, Management, Magerit, CRAMM, Information Technology, IT, Information Security, ISMS.

Fuente imagen: www.ej2informatica.com

Introducción

El presente trabajo realiza una comparación entre las metodologías MAGERIT y CRAMM, utilizadas para el análisis y gestión de riesgos de la seguridad de la información, en base a mecanismos de identificación de activos, identificación de vulnerabilidades, funciones de probabilidad, variable de medición de riesgo y cálculo de riesgo.

De esta manera se identifica la metodología más adecuada que será utilizada en la gestión de riesgo tecnológico en las MPYMES ecuatorianas. Muchos responsables de sistemas de información deberán crear conciencia de la existencia de riesgos y de la gran necesidad de mitigar cada una de las vulnerabilidades que día a día se presentan en el sistema.

Este documento presenta una comparación entre Magerit y CRAMM; en la que define la metodología más adecuada para utilizarse en las MPYMES ecuatorianas. Hay que aclarar que en primera instancia, estas metodologías deben estar alineadas con las normas internacionales ISO 27001, 27002, 27005 y 31000.

Las MPYMES ecuatorianas están inmersas en un eminente entorno de riesgo, ya sea a nivel nacional por la inestabilidad política y/o económica; o regional debido a las condiciones naturales en las que se asienta cada ciudad. Además consideran que la informática es solamente un área de soporte, y que la inversión en elementos y mecanismos de seguridad convergen solamente en una solución antivirus. El desconocimiento, la exigencia y extensión de las normas, ayudan a que el concepto de gestión de riesgo informático quede como un mito empresarial.

Metodología

La metodología empleada se basa en un proceso de razonamiento que intenta no sólo describir cada hecho, sino a la par presentar explicaciones de cada uno de los elementos trabajados.

El ministerio de Hacienda y Administraciones Públicas de España, ha definido a Magerit como

> “Una metodología que ha sido elaborada como respuesta a la percepción de la administración pública (y en general toda la sociedad) depende de forma creciente de los sistemas de información para alcanzar sus objetivos. Así, menciona que el uso de tecnologías de la información y comunicaciones (TIC) supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben gestionarse prudentemente con medidas de seguridad que sustenten la confianza de los usuarios de los servicios” (Ministerio de Hacienda y Administraciones Públicas de España, 2012).

Por otro lado Geovanna Cordero acota que: Magerit está directamente relacionada con la generalización del uso de las tecnologías de la información. Por lo tanto se puede decir que es un instrumento que facilita la implantación y aplicación del esquema nacional de seguridad de España, proporcionando los principios básicos y requisitos

mínimos para la protección de la información. Desde otro punto de vista, la gestión de riesgos consiste en el proceso de analizar, evaluar, tratar, monitorizar y comunicar los riesgos encontrados (Cocho, 2006).

La otra metodología analizada, CRAMM, fue desarrollada en 1985 en el Reino Unido por la Agencia Central de Cómputo y Telecomunicaciones, y estaba destinada a proteger la confidencialidad, integridad y disponibilidad de un sistema de información y sus activos; y se define como una metodología para el análisis y gestión de riesgos, orientada a proteger la confidencialidad, la integridad y disponibilidad de un sistema y sus activos, que puede ser aplicable en todo tipo de sistemas y redes de información en la etapa de estudio de factibilidad; donde el alto nivel del riesgo puede ser requerido para identificar los requisitos de seguridad general, la contingencia y los costos asociados de las distintas opciones (Yazar, 2002) (Cordero Torres, 2015).

Esta investigación proporciona como resultado, un análisis comparativo de las metodologías Magerit y CRAMM, en base a mecanismos para la identificación de activos, identificación de vulnerabilidades, funciones de probabilidad, variable de medición de riesgo y cálculo de riesgo.

Toda metodología de gestión de riesgo parte desde la identificación de la información que se quiere proteger, conocidas como activos de información; que comprende el hardware, el software y los elementos que contienen información. El segundo paso es identificar los riesgos y amenazas del entorno, para continuar luego con la identificación de los mecanismos o contramedidas que permitirán reducir el impacto.

La investigación

La seguridad de la información y el riesgo informático

Existen múltiples definiciones para la seguridad de la información. Una de ellas es: “la protección contra todos los daños sufridos o causados por la herramienta informática y originados por el acto voluntario y de mala fe de un individuo” (Royer, 2004)

Para Germán Alcides el riesgo informático es un conjunto de normas y procedimientos que son aplicados para salvaguardar un sistema informático, cuya finalidad es garantizar que todos los recursos que conforman el sistema informático sean utilizados para el fin que fueron creados sin ninguna intromisión (Alcides, 2009).

De las definiciones anteriores se desprende que la seguridad de la información se fundamenta en tres principios básicos: confidencialidad, disponibilidad e integridad; entendiéndose por confidencialidad a los mecanismos que garantizan el acceso a la información a personas y organismos autorizados, por integridad a la consistencia de la información almacenada, y por disponibilidad a la característica de que la información debe estar disponible en el momento que sea requerida.
La seguridad de la información contempla como actores a los elemen-

tos que de una u otra forma están involucrados con el manejo de la información, tanto digital como física dentro de una organización. Así por ejemplo, la metodología Magerit contempla al hardware, software, información electrónica, recurso humano, entre otros, como actores que consumen y producen información.

La información, para cualquier organización, ya sea pública o privada, tiene valor monetario. Por ejemplo, para el Servicio de Rentas Internas, la base de datos de sus contribuyentes es esencial, o la base de datos de los sujetos de crédito para un banco son muy importantes. Las instituciones, organismos y empresas deben preguntarse: ¿Cuánto vale esa información para mi organización, y cuánto para mi competencia? La información esencial puede ser un objetivo muy atractivo para un tercero, y muchas veces, por descuido o por desconocimiento, la misma puede verse comprometida.

La vulnerabilidad hace referencia a las debilidades que existen en un sistema de información, lo que permite que pueda ser fácilmente atacado, evadiendo el control de acceso y la confidencialidad de los datos y las aplicaciones existentes (Cordero Torres, 2015). Las vulnerabilidades deben ser expresadas en una escala numérica para poder posteriormente cuantificar su impacto, y, citando a Burgos y Campos, se sugiere que éstas sean identificadas y valoradas individualmente (Cordero Torres, 2015) (Burgos Salazar & Campos, 2008).
La vulnerabilidad, de acuerdo a Pablo Castaño, debe ser expresada mediante la fórmula básica:

Vulnerabilidad=Frecuencia estimada / Días al año (Cordero Torres, 2015) (Castaño, 2014)

Esto significa que la vulnerabilidad se da por el número de ocurrencias que puedan presentarse en un tiempo. Así Castaño sugiere la siguiente escala de frecuencias de repetición y el tipo de vulnerabilidad presentada.

Tabla 1: Vulnerabilidades y frecuencias

Vulnerabilidad	Rango	Valor
Frecuencia extrema	1 vez al día	1
Frecuencia alta	1 vez cada dos semanas	26/365 = 0.071
Frecuencia media	1 vez cada dos meses	0.016
Frecuencia baja	1 vez cada 6 meses	0.005
Frecuencia muy baja	1 vez al año	0.002

Fuente: (Castaño, 2014)

Las amenazas son los elementos que pueden dañar o alterar la información de una u otra forma. Estas generalmente pueden ser encontradas a partir de una vulnerabilidad existente. El riesgo a su vez, es la probabilidad que tiene una amenaza para originarse y que puede generar un cierto impacto en la organización.

Los marcos de referencia internacionales utilizados en la gestión de riesgo

Con el objetivo de estandarizar los procesos y actividades para la gestión de riesgo, la Organización Internacional para Estandarización (ISO) agrupa a las mejores prácticas de la industria en la familia ISO 27000, a manera de aconsejar a las organizaciones en el desarrollo, implementación y administración de un sistema de gestión de seguridad de la información o SGSI. A continuación se detallan los estándares que pertenecen a la familia ISO 27000.

ISO 27001

Publicada el 15 de octubre de 2005, y basada en el modelo de Deming, proporciona un modelo para establecer, implementar, operar, supervisar, revisar, mantener y mejorar un sistema de gestión de seguridad de la información. El marco referencial es aplicable a todo tipo de organización, pues es bastante extensa en cuanto a su aplicación y controles operacionales.

La ISO 27001 está constituida por los siguientes dominios:

- La política de seguridad, cuyo objetivo es garantizar el soporte y gestión necesarios para la seguridad, según los requisitos institucionales y normativos.

- La organización de la seguridad de la información, cuya finalidad es instaurar un marco de referencia para la implementación y control de la seguridad de la información.

- La gestión de activos, que tiene como objetivo asegurar los activos de la organización.

- La seguridad de los recursos humanos, cuyo objetivo es fijar las medidas necesarias para controlar la seguridad de la información, que sea manejada por los recursos humanos.

- La seguridad física y del ambiente, que busca proteger a las instalaciones de la organización y a toda la información que maneja.

- La gestión de las comunicaciones y operaciones, que permite determinar el procedimiento y responsabilidades de las operaciones que realiza la organización.

- El control de acceso, con el que se asegura la confidencialidad de los sistemas de información de la organización.

- La adquisición, desarrollo y mantenimiento de los sistemas de información, dirigida a organizaciones que desarrollen software internamente o que tengan un contrato con otra organización que sea la encargada de desarrollarlo.

- La gestión de incidentes en la seguridad de la información, que aplica un proceso de mejora constante en la gestión de percances de seguridad de la información.

- La gestión de la continuidad del negocio, cuyo objetivo es garantizar la continuidad operativa de la organización.

- El cumplimiento, que busca asegurar que los requisitos legales de seguridad referidos al diseño, operación, uso y gestión de los sistemas de información se cumplan (Cordero Torres, 2015).

ISO/IEC 27002:2005:

Establece directrices y principios generales para la iniciación, implementación, mantenimiento y mejora de la gestión de seguridad de la información en una organización. Está estructurada en 16 capítulos (27001 Academy, 2015), los mismos que se citan a continuación:

- Conceptos generales: Fundamentos de seguridad de la información y SGSI.

- Campo de aplicación: capítulo que especifica el objetivo de la norma y su campo de aplicación.

- Términos y definiciones: contiene una breve descripción de los términos más usados en la norma.

- Estructura del estándar: describe la estructura de la norma.

- La evaluación y tratamiento del riesgo: incluye procedimientos y detalles sobre evaluación y tratamiento de los riesgos de seguridad de la información.

- La política de seguridad: presenta los mecanismos para establecer controles que permitan orientar a la alta dirección sobre la seguridad de la información.

- La gestión de activos: da las pautas para establecer controles que permitan lograr y mantener la protección adecuada de los activos de información de la organización.

- Seguridad ligada a los recursos humanos: recomienda controles para el aseguramiento de los empleados, contratistas y usuarios de terceras partes.

- Seguridad física y ambiental: proporciona controles que permitan evitar el acceso físico no autorizado, el daño o la interferencia en las instalaciones y a la información de la organización, de igual forma evitar la pérdida, daño, robo o puesta en peligro de los activos, y la interrupción de las actividades de la organización.

- La gestión de comunicaciones y operaciones: orientada al establecimiento de controles que permitan asegurar la operación correcta y segura de los servicios de procesamiento de información e implementar y mantener un grado adecuado de seguridad de la

información, de la prestación del servicio, de conformidad con los acuerdos de prestación del servicio por terceros.

- El control de acceso: con prácticas que permitan controlar el acceso a la información de la organización con base en los requisitos de seguridad y del negocio, y asegurar la confidencialidad de los sistemas de información.

- La adquisición, desarrollo y mantenimiento de los sistemas de información: su objetivo es proporcionar lineamientos que garanticen la seguridad en los procesos de adquisición, mantenimiento y desarrollo del software.

- La gestión de incidentes de seguridad de la información: propone controles que permitan asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información, y la forma de comunicar.

- La gestión de la continuidad del negocio: propone controles orientados a contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra fallos y desastres.

- El cumplimiento: donde se establecen controles de cumplimiento legal, obligaciones estatuarias reglamentarias o contractuales y de cualquier requisito de seguridad (Cordero Torres, 2015).

ISO/IEC 27005:2011

Esta norma es compatible con los conceptos generales especificados en la norma ISO/IEC 27001; contiene la descripción de los procesos para la gestión del riesgo en la seguridad de la información y sus actividades y proporciona directrices para gestión de riesgos. Está pensada para ser aplicada en todo tipo de organizaciones que tienen la intención de gestionar los riesgos que podrían comprometer la seguridad de la información de la organización (Cordero Torres, 2015).

ISO 31000:2009

Esta norma hace referencia a la gestión del riesgo, brindando principios y directrices. Esta norma proporciona directrices sobre cómo se debe establecer y mantener un marco de gestión de riesgos, el mismo que puede ser adoptado por cualquier organización (Cordero Torres, 2015).

Estudio comparativo de las metodologías Magerit y CRAMM

Considerando las necesidades de las MPYMES ecuatorianas, ambas metodologías establecen como objetivo principal la gestión y análisis de riesgo; son distribuidas de forma gratuita en idioma inglés, pero Magerit, además, está disponible en idioma español. Uno de los inconvenientes es que CRAMM está enfocada al uso en organizaciones e instituciones grandes, por cuanto difícilmente podría encajar en la

gestión de riesgo tecnológico de las MPYMES ecuatorianas.

Las herramientas que apoyan a la metodología Magerit para la gestión de riesgo son Pilar y EAR, la primera de distribución libre. Para CRAMM, las herramientas para la gestión de riesgo son comerciales. Cada metodología está alineada a estándares internacionales. Magerit adopta las mejores prácticas de la ISO 27001, 15408, 17799, y 13335. Sin embargo para la gestión de riesgos se alinea correctamente con los requerimientos de la ISO 27005 e ISO 31000. CRAMM, a su vez, tiene un enfoque más práctico, pues su base de referencia es la ISO 27002, y contempla además los fundamentos de la ISO 27005 e ISO 31000.

El ciclo de Magerit inicia con la identificación de los activos de información, luego identifica las amenazas lógicas y de entorno, estima las frecuencias y el impacto para inmediatamente pasar a las salvaguardas y gestionar finalmente el riesgo residual. El ciclo de CRAMM consiste primero en identificar los riesgos y luego estimar la frecuencia de presentación de los mismos.

Magerit considera como activos de información al hardware, software, información electrónica, personas, instalaciones, medios de soporte y elementos de comunicación de datos. CRAMM a su vez, considera como activo de información solamente a los datos.

CRAMM utiliza solamente métodos cualitativos y cuantitativos para la identificación de riesgos y amenazas; además de valorar a los activos por términos de costo de reemplazo, y por dimensiones de disponibilidad, integridad y confidencialidad. Magerit utiliza además de los dos métodos, el método mixto. Además determina el valor de los activos considerando la dimensión de disponibilidad, integridad, confidencialidad, trazabilidad y autenticidad, y estableciendo una escala de valoración en seis niveles: Muy alto, alto, medio, bajo, muy bajo y despreciable.

Magerit analiza el impacto determinando el valor de los activos, el impacto acumulado lo calcula considerando el valor acumulado del activo y las amenazas a las que se afronta, y el impacto repercutido considerando el valor propio y las amenazas.

MAGERIT, basado en la ISO 27005 e ISO 31000, gestiona los riesgos mediante la aplicación de salvaguardas, las mismas que se clasifican en: protecciones generales, protección de claves, protección de los servicios, protección del software, hardware y comunicaciones. CRAMM se alinea con el estándar ISO 27005 en su fase de planificación donde se realiza la identificación y evaluación del riesgo; y con la ISO 31000 para valorar y dimensionar el riesgo como para establecer una contramedida.

Conclusiones

Al finalizar este proyecto de investigación se observa que tanto MAGERIT como CRAMM son metodologías bastante similares, que permiten identificar los riesgos y amenazas que podrían afectar en integridad,

confidencialidad y disponibilidad de información, y a la vez permiten tomar medidas de salvaguardia con lo que se obtiene como resultado la disminución de tiempo.

Ambas llevan a una identificación de los activos, inventarios de los mismos, amenazas, impacto y probabilidad obteniendo como resultado salvaguardias para minimizar el riesgo. La diferencia principal que existe entre MAGERIT y CRAMM está en que la primera desarrolla procesos para su implementación dentro de la planificación y lanzamiento de un proyecto lo que da resultados de pérdida o ganancia económica y CRAMM se aplica directamente para las organizaciones y los resultados se evalúan en una tabla con ponderación de 1 a 7.

En el contexto de las MPYMES ecuatorianas, Magerit es la metodología que podría ser aplicada. La ventaja principal es que primero busca “qué” se quiere proteger, luego establece el “de qué” se quiere proteger, para finalmente decidir el “cómo” se debe proteger. Sin embargo es inconclusa, ya que llega solamente a las pautas a considerar para establecer las contramedidas. Es importante mencionar que la implementación de un sistema de gestión de seguridad de la información debería introducirse en las políticas de seguridad, y considerar la continuidad del negocio en un ciclo infinito de planificación, ejecución, verificación y actuación.

Referencias bibliográficas

- 27001 Academy. (2015). 27001 academy. Obtenido de http://www.iso27001standard.com/es/que-es-iso-27001/
- Alcides, G. (2009). Seguridad informática. Antioquía, Colombia: Universidad de Antioquía.
- Auditoria, Informática, Fraudes, CAATTs. (07 de 08 de 2014). Obtenido de http://fraudit.blogspot.com/2008/07/la-familia-iso-27000.html
- Burgos Salazar, J., & Campos, P. G. (2008). Modelo Para Seguridad de la Información en TIC. Concepción, Chile: Universidad del Bío-Bío.
- Castaño, P. (7 de Septiembre de 2014). Metodología de Análisis de Riesgos: MAGERIT. Obtenido de GR2DEST: http://blacksecurity.net/Gr2Dest/metodologia-de-analisis-de-riesgos-magerit/
- CGEIT, C. C. (20 de 09 de 2014). CIGRAS. Obtenido de http://www.isaca.org/chapters8/Montevideo/cigras/Documents/cigras2011-cserra-presentacion1%20modo%20de%20compatibilidad.pdf
- Cocho, J. M. (Junio de 2006). MAGERIT Y LA NORMALIZACIÓN DE OTROS MODELOS. Sevilla, España.
- Cordero Torres, G. (01 de 07 de 2015). Estudio comparativo entre las metodologías MAGERIT y CRAMM, utilizadas para análisis y gestión de riesgos de seguridad de la información. Cuenca, Azuay, Ecuador.
- Dirección General de Modernización Administrativa, P. e. (2012). MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. . Madrid.
- G2D. (22 de 09 de 2014). GR2DEST.ORG. Obtenido de http://gr2dest.org/metodologia-de-analisis-de-riesgos-magerit/
- Gestión de la información. (s.f.). Obtenido de http://arelyromero.blogspot.com/2012/11/de-nuevo-nos-concentramos-en-el.html
- ISO. (s.f.). Obtenido de http://www.iso.org/iso/catalogue_detail?csnumber=43170
- Ltd, I. (s.f.). Information security standards. Obtenido de http://www.iso27001security.com/html/27005.html
- Ministerio de Hacienda y Administraciones Públicas de España. (Octubre de 2012). Magerit 3. Madrid, España.
- Morales, R. (25 de 07 de 2014). RETRIC. Obtenido de RETRIC: http://retico.gt/2013/10/09/principios-de-la-seguridad-informatica-2/
- Ormella, I. C. (22 de 09 de 2014). Norma ISO 31000 de Riesgos Corporativos. Obtenido de http://www.criptored.upm.es/descarga/ISO_31000_riesgos_corporativos.pdf
- Portal Administración Electrónica de España. (22 de 01 de 2015). Obtenido de http://administracionelectronica.gob.es/ctt/magerit#.VMGxmpbRbHQ
- Royer, J.-M. (2004). Seguridad en la Informática de Empresa: riesgos, amenazas, prevención y soluciones. Barcelona: Eni ediciones.
- Seguridad Informatica. (s.f.). Recuperado el 28 de 05 de 2015, de http://seguridadinformaticaufps.wikispaces.com/Herramienta+de+Evaluacion+de+Riesgo-CRAMM
- Seguridad Informatica. (11 de 05 de 2015). Obtenido de https://seguridadinformaticaufps.wikispaces.com/Herramienta+de+Evaluacion+de+Riesgo-CRAMM
- SUSCERTE. (07 de 08 de 2014). Obtenido de http://www.sunai.gob.ve/images/stories/PDF/Ponencias/EF/3_Daniel_sandoval.pdf
- Yazar, Z. (2002). A qualitative risk analysis and management tool – CRAMM. Information Security Reading Room., 6. SANS Institute.