Integración de la Gestión de Riesgos en entornos de TI

Béatrix Barafort[1], Antoni-Lluís Mesquida[2], Antonia Mas[2]

[1]Luxembourg Institute of Science and Technology, 5 Avenue des Hauts-Fourneaux, L-4362 Esch-sur-Alzette, Luxembourg
[2]Department of Mathematics and Computer Science, University of the Balearic Islands, Ctra. de Valldemossa, km. 7.5, E07122 Palma de Mallorca, Spain
beatrix.barafort@list.lu, antoni.mesquida@uib.es, antonia.mas@uib.es

Resumen. Este artículo analiza las actividades de gestión de riesgos recogidas en varios estándares ISO para así proporcionar una base para mejorar, coordinar e interoperar las actividades de gestión de riesgos en entornos de TI. Tomando como base el estándar internacional ISO 31000 para la gestión de riesgos, se realiza un análisis comparativo de las siguientes normas con el objetivo de identificar las actividades relacionadas con la gestión de riesgos: ISO high level structure for management system standards, ISO 9001 Requisitos de un sistema de gestión de la calidad, ISO 21500 Guía para la gestión de proyectos, ISO/IEC 20000-1 Requisitos de un sistema de gestión de servicios de TI e ISO/IEC 27001 Sistema de gestión de la seguridad de la información de TI. Estas normas facilitan la integración de todas las actividades basadas en procesos, así como la implementación de mecanismos para alinear a todas las entidades de la organización, con el objetivo de hacer frente a los desafíos relacionados con la gestión de riesgos. Se presentan diferentes perspectivas de integración como pueden ser la comprensión de la organización y su contexto, el pensamiento basado en el riesgo, el liderazgo y el compromiso, el enfoque basado en procesos y la estructura PDCA.

Palabras clave: Gestión integrada de riesgos; Sistema de gestión integrado; Entornos de TI; Estándares ISO

Béatrix Barafort, Antoni-Lluís Mesquida, Antonia Mas, Integrating risk management in IT settings from ISO standards and management systems perspectives, Computer Standards & Interfaces, Available online 30 November 2016, ISSN 0920-5489. (DOI: 10.1016/j.csi.2016.11.010)