Sistema de evaluación para la reducción de la incertidumbre de las tipologías y taxonomías de la norma ISO/IEC 27001 en la industria 4.0

Evaluation system for the reduction of uncertainty of ISO/IEC 27001 typologies and taxonomies in industry 4.0

Juan Vicente Barraza de la Paz[a]*, Luis Alberto Rodríguez Picón[a]
[a]Departamento de Ingeniería Industrial y Manufactura, Doctorado en Tecnología, , Instituto de Ingeniería y Tecnología, Universidad Autónoma de Ciudad Juárez, Chihuahua, México.
*Autor de correspondencia. Correo electrónico: al216655@alumnos.uacj.mx

No. de resumen
4CP22-13

Formato
Ponencia

Evento
4.º Coloquio de Posgrados IIT

Presentador
Juan Vicente Barraza de la Paz

Tema
Cómputo Aplicado

Estatus
Estudio en curso

Fecha de la presentación
Noviembre 25, 2022

Resumen

El uso cada vez más frecuente de diferentes dispositivos que traen consigo la I4.0 así como el IoT y los sistemas de información presentes en los diferentes procesos de las empresas, ofrece grandes ventajas competidas, pero estas no vienen exentas de riesgos. Si bien la ISO/IEC 27001 proporciona los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información, permitiendo evaluar los riesgos a la que está expuesta la información periódicamente, la evaluación de riesgos debería ser un proceso de análisis en tiempo real y no lineal, por lo que los enfoques actuales no son adecuados, y aun cuando se ha identificado en la revisión de literatura una creciente tendencia de publicaciones esta se encuentra en desarrollo. Por tanto, la presente investigación realiza una revisión sistemática de las principales metodologías de gestión de riesgos, identificando sus tipologías y taxonomías, donde metodologías de gestión de riesgos con características de evaluación cuantitativas y cualitativas, como la de NIST, ISO27005, MAGERIT o IRAM, varían tanto en forma como en estructura, donde la mayoría de estas cumplen con lo siguiente una aplicación sistemática de políticas, procedimientos y prácticas a las actividades de comunicación y consulta, un conjunto procesos de evaluación del riesgo que implica una preparación de la evaluación de riesgos, evaluación de factores de riesgos, determinación o valoración de riesgo y control o tratamiento de riesgos, convirtiendo a la gestión de riesgos en un diferenciador el cual genera confianza en clientes y proveedores.

Palabras clave: ISO27001, gestión de riesgos, NIST, ISO27005, MAGERIT.

Abstract

The increasingly frequent use of different devices that bring with them the I4.0 as well as the IoT, and the information systems present in the different processes of companies, offers great competitive advantages, but these advantages do not come without risks. Although the ISO/IEC 27001 provides the requirements to establish, implement, maintain and continuously improve an information security management system, allowing to evaluate the risks to which the information is exposed periodically, risk assessment should be a process of analysis in real time and not linear, so the current approaches are not adequate, and even when it has been identified in the literature review a growing trend of publications, these approaches are under development. Therefore, the present research performs a systematic review of the main risk management methodologies, identifying their typologies and taxon-

omies, where risk management methodologies with quantitative and qualitative assessment characteristics such as NIST, ISO27005, MAGERIT or IRAM, vary both in form and structure, where most of these comply with the following a systematic application of policies, procedures and practices to communication and consultation activities, a process of risk assessment processes: which involves preparation of risk assessment, evaluation of risk factors, determination or assessment of risk and control or treatment of risk. Turning risk management into a differentiator which generates confidence in customers and suppliers.

Keywords: ISO27001, risk management, NIST, ISO27005, MAGERIT.

Entidad legal responsable del estudio

Universidad Autónoma de Ciudad Juárez

Financiamiento

Beca de posgrado CONACYT.

Conflictos de interés

Los autores declaran que no existe conflicto de intereses.