

Procedimiento para evaluar los riesgos del cumplimiento normativo en organizaciones orientadas a proyectos

Procedure to assess compliance risks in project-oriented organizations

Yasmany Aguilera Sánchez¹, Juan Antonio Plasencia Soler², Fernando Marrero Delgado³

Universidad de las Ciencias Informáticas, La Habana, Cuba
Universidad Central de Las Villas “Martha Abreu de las Villas”, Las Villas, Cuba

Datos de los autores

¹ Ingeniero en Ciencias Informáticas, Profesor instructor, Universidad de las Ciencias Informáticas, La Habana, Cuba. yasmanyas@uci.cu

² Doctor en Ciencias, Profesor Auxiliar, Universidad de las Ciencias Informáticas, La Habana, Cuba juanps@uci.cu

³ Doctor en Ciencias, Profesor Titular, Universidad Central de Las Villas “Martha Abreu de las Villas”, Las Villas, Cuba. fmarrero@uclv.edu.cu

RESUMEN

Introducción: La correcta identificación y evaluación de los riesgos se está convirtiendo en un elemento crucial en la gestión de las organizaciones. Llevar a cabo los programas de cumplimiento normativo mediante la gestión de riesgos de compliance, posibilita integrar herramientas de gestión para el logro de la sostenibilidad organizacional.

Objetivo: Desarrollar un procedimiento para la evaluación de riesgos de cumplimiento normativo.

Métodos: Se tuvo en cuenta las normas Internacionales (ISO 19600: 2014, NC-ISO 9001 del 2015 y NC-ISO 31000 del 2018) sobre los sistemas de gestión del cumplimiento normativo y la Resolución 60 del Control Interno de la Contraloría General de la República de Cuba. Se aplicaron entrevistas y encuestas, participaron un total de 28 trabajadores de la entidad en estudio. Se aplicó el método de expertos para la validación del procedimiento.

Resultados: Se identificaron y validaron 14 riesgos del proceso de recursos humanos y se diseñó el procedimiento para evaluar los riesgos de cumplimiento normativo en organizaciones orientadas a proyectos, el cual se describe en 4 pasos.

Conclusiones: La incorporación de este procedimiento a la gestión de riesgos del cumplimiento ético y normativo permite a la organización, desde la gestión de riesgos, identificar las deficiencias de las actividades de los procesos de la organización, asociadas al cumplimiento legal, ético y normativo y permite mejorar los indicadores del desempeño organizacional.

PALABRAS CLAVE: programa de ética y compliance; gestión de riesgos; índice de criticidad

ABSTRACT

Introduction: The correct identification and evaluation of risks is becoming a crucial element in the management of organizations. Carrying out regulatory compliance programs through the management of compliance risks makes it possible to integrate management tools for the achievement of organizational sustainability.

Objective: To develop a procedure for the evaluation of regulatory compliance risks.

Methods: The International Standard: ISO 19600: 2014, NC-ISO 9001: 2015, NC-ISO 31000: 2018 and on the compliance management systems and Resolution 60 of the Internal Control of the General Comptroller of the Republic of Cuba were taken into account. Interviews and surveys were applied, a total of 28 workers of the entity under study participated. The expert method was applied for the validation of the procedure.

Results: We identified and validated 14 risks of the human resources process and designed the procedure to evaluate the risks of regulatory compliance in project-oriented organizations, which is described in 4 steps.

Conclusions: The incorporation of this procedure to the risk management of ethical and regulatory compliance allows the organization, from risk management, to identify the deficiencies of the activities of the organization's processes, associated with legal, ethical and regulatory compliance and it allows improving the indicators of organizational performance.

KEYWORDS: ethics and compliance program; risk management; criticality index

RECIBIDO: 06/02/2019

APROBADO: 20/05/2019

INTRODUCCIÓN

Desde la publicación del primer estándar de gestión de cumplimiento normativo en el año 2006 por el Organismo de Normalización Australiano (SA), la Norma AS 3806, se han incrementados sus aplicaciones en las organizaciones, hasta que, en el año 2014, la Organización Internacional de Normalización (ISO) desarrolló la Norma ISO 19600:2015, Sistema de Gestión de Cumplimiento Normativo. Esta guía de referencia internacional otorga a las organizaciones de un sistema eficaz de gestión de cumplimiento con lo normado, y que tienen como principal objetivo la mitigación de este tipo de riesgos.

La ISO 19600 propone un conjunto de directrices con la finalidad de proporcionar disposiciones sobre cómo establecer, desarrollar, ejecutar, evaluar, mantener y mejorar un sistema eficaz de

gestión de cumplimiento dentro de la organización, por lo que no es una norma certificable; en consecuencia, el alcance de los requisitos depende del tamaño, la estructura, la naturaleza y complejidad de la organización (ISO-19600, 2014).

Las investigaciones (Cordero Morales D. & Torres Rubio Y., 2013; Pérez Moya O., 2013; Hernández Díaz N. & Cuza García B., 2013; Bolaño-Rodríguez Y., 2014; Martell-Fernández V., 2014; ISO, 2018; Vargas Aguila, Aguila, Perez, Rodríguez, & Fumero, 2017; Martínez, 2017) realizan aportes a la conceptualización de los riesgos desde las más diversas aristas, lo cual ha permitido obtener diferentes definiciones de un mismo concepto. El riesgo es definido entonces como el efecto de la incertidumbre sobre los objetivos de una organización y medido por sus consecuencias, su probabilidad de ocurrencia y su nivel de detección.

MÉTODOS

La metodología aplicada fue la siguiente:

- Se tuvo en cuenta la Norma Internacional ISO 19600: 2014 sobre los sistemas de gestión del cumplimiento normativo y la Resolución 60 del Control Interno de la Contaduría General de la República de Cuba, así como la NC-ISO 9001 del 2015 Sistema de gestión de la Calidad y la NC-ISO 31000 del 2018 Gestión de riesgos: Directrices.
- Mediante un ciclo de Deming o ciclo PHCA (Planear, Hacer, Actuar, Controlar), se diseñó un procedimiento para la evaluación de los riesgos de cumplimiento normativo. (Figura 1)

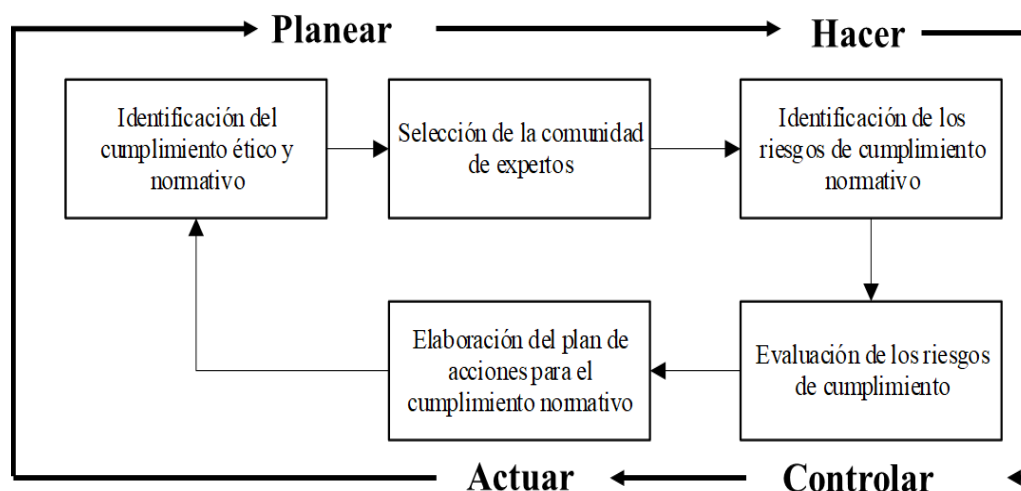


Figura 1: Modelo para la evaluación de los riesgos de cumplimiento normativo.

Fuente: Elaboración propia

- Se aplicaron encuestas y entrevistas a especialistas para identificar los riesgos, así como el marco legal y ético asociado a los mismos. Se entrevistaron 28 trabajadores.

- Entre las principales interrogantes del instrumento aplicado para el diagnóstico estratégico resultaron:
 - La organización define objetivos, indicadores y metas económicas, sociales y ambientales en el corto, mediano y largo plazo teniendo en cuenta los requerimientos de los grupos de interés.
 - La organización desarrolla productos y servicios encaminados a resolver cuestiones sociales, ambientales y éticas.
 - La organización contribuye a través de sus productos y servicios a la sustitución de importaciones.
 - La organización garantiza las condiciones requeridas de seguridad, salud e higiene del trabajo avalada por los buenos resultados en estudios de satisfacción.
- Se calculó el índice de criticidad de los riesgos a partir de la propuesta de Plasencia-Soler, (2018), con el empleo de la siguiente ecuación (1):

$$Ic_i = P_i * Imax_i(Eco_i; Soc_i; Ecol_i) \quad (1)$$

Donde:

P_i : Probabilidad de ocurrencia del riesgo (i).

$Imax_i$: Valor máximo del impacto luego de evaluar el riesgo (i) en las dimensiones: económica, social, ecológica.

Para este paso se utiliza la escala propuesta en la tabla 1.

- Se aplicó el método de expertos, con la participación de 7 expertos para validación del procedimiento.
- Para la evaluación de los riesgos se tuvo en cuenta la siguiente escala:

Tabla 1: Escala de evaluación de los riesgos

Valor	Impacto	Probabilidad
5	Catastrófico	Muy alta
4	Crítico	Alta
3	Moderado	Moderada
2	Menor	Baja
1	Insignificante	Remota

Fuente: Adaptado de Plasencia-Soler, 2018

RESULTADOS

La dirección de la organización identificó de conjunto con la comunidad de expertos el marco legal, ético y normativo asociado al proceso seleccionado y se capacitó a los siete expertos que realizarían la definición y evaluación de los riesgos. A continuación se detallan los riesgos del proceso de recursos humanos en la organización validados por los expertos. (Tabla 2).

Tabla 2: Riesgos de compliance del proceso de Gestión de los Recursos Humanos

Código del Riesgo	Marco Legal y ético	Descripción del Riesgo
R01	Código del Trabajo	Elaboración deficiente de las prenomas.
R02		Incumplimiento de la medida disciplinaria.
R03		Inadecuado levantamiento de necesidades de capacitación.
R04		Trabajadores con títulos de cursos de los que no son matrícula.
R05		Entrega de un expediente laboral al trabajador indebidamente.
R06		Contratación de personal no idóneo para la plaza.
R07	Decreto 339 y 340/2016	Modificaciones de períodos de maternidad.
R08	Res 283/2009	Inadecuado cálculo de años de servicio de un trabajador para la jubilación.
R09	Código de Ética	Inadecuado uso del acceso a internet.
R10	NC-ISO 45001/2018 Sistema de Gestión de la Seguridad y Salud en el Trabajo.	Accidentes o enfermedades profesionales de los trabajadores.
R11	Res 85/2016	Entrega de certificado de categoría docente erróneamente.
R12	Res 43/2012	Desconocimiento por parte del jefe de los verdaderos motivos de ausencia de un trabajador.
R13	Res 9/2016	Inadecuado sistema de pago a trabajadores.
R14	Res 95/2017	Inadecuada entrega de estimulación.

Fuente: Elaboración propia.

Los riesgos identificados fueron evaluados por la comunidad de expertos por consenso. Luego se calculó el Índice de Criticidad (Ic) de los riesgos a través de la ecuación (1).

De acuerdo a la priorización de los riesgos fueron implementados acciones de control para reducir sus impactos en la organización. La Figura 2 muestra la variación del índice de criticidad luego de aplicadas las medidas para su mitigación o el índice residual de los riesgos fundamentales.

En la Figura 3 se recogen los resultados de la evaluación de los riesgos, evidenciando la diferencia del impacto de los riesgos en la dimensión ambiental respecto al resto de las dimensiones.

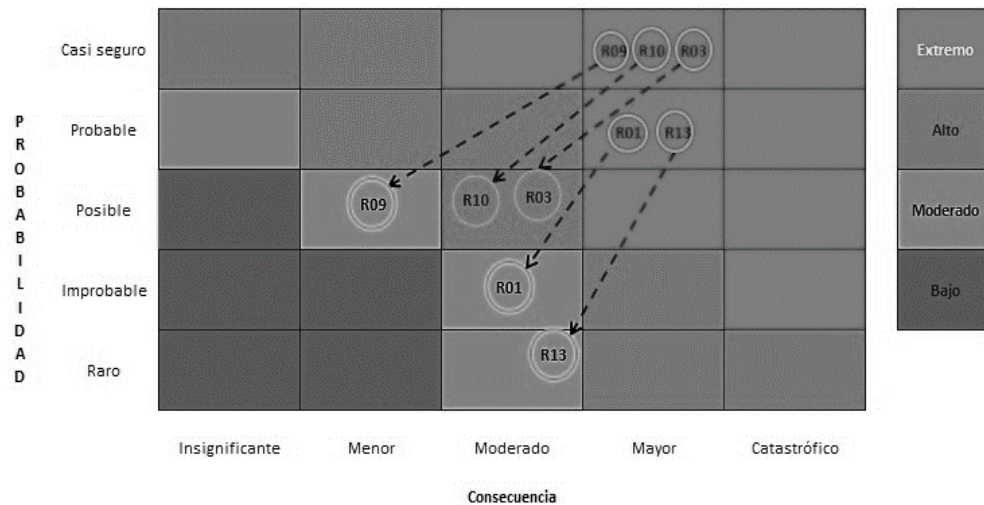


Figura 2: Mapa de riesgos residuales

Fuente: Elaboración propia

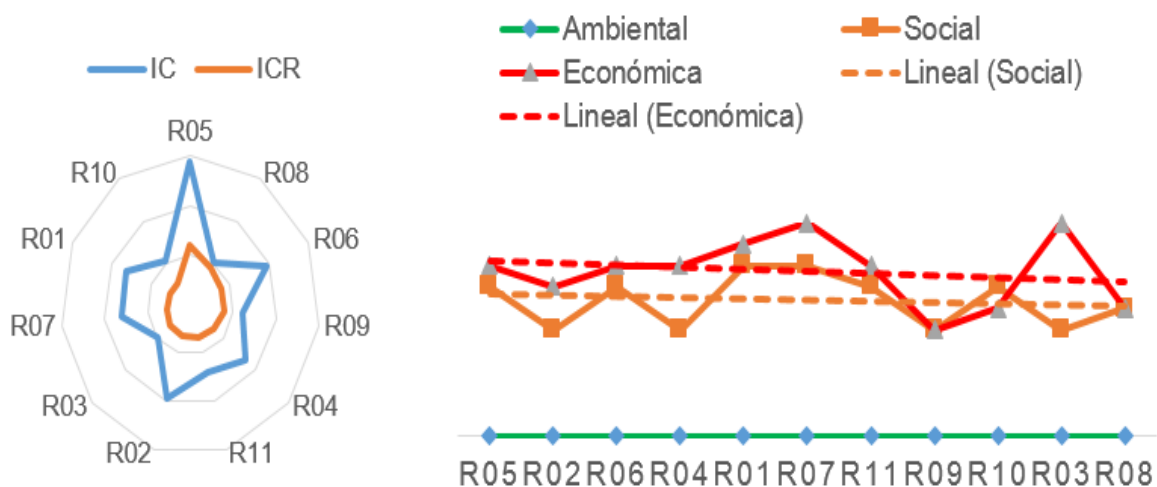


Figura 3 : Resultados de la evaluación de los riesgos

Fuente: Elaboración propia

Se obtuvo el siguiente procedimiento:

Paso 1. Identificación del cumplimiento ético y normativo

En este paso se identificó y documentó, de manera sistemática, las obligaciones de la organización. Estas obligaciones provienen de normas y resoluciones relevantes para la organización y el sector al que pertenece; reglas o guías emitidas por agencias regulatorias; tratados, convenios y protocolos; acuerdos con grupos de la comunidad; compromisos ambientales; leyes y decretos ley, entre otros desde el punto de vista externo. Desde el punto de vista interno, las políticas, códigos, normas y otras obligaciones que rigen el comportamiento de la organización. Es importante disponer de canales de comunicación que identifiquen novedades y modificaciones en las obligaciones para asegurar un cumplimiento continuo.

Paso 2. Selección de los Expertos

El trabajo con expertos es de vital importancia durante todo el procedimiento, son estos los que deberán realizar las evaluaciones de los criterios que componen el índice de criticidad, así como también pueden ser utilizados en la determinación de los pesos asociados a los criterios.

Paso 3. Identificación de los riesgos de cumplimiento normativo

En este paso se identificaron los riesgos de “compliance” (Traducción al español: riesgos de cumplimiento normativo) asociados con el cumplimiento ético-legal. Estas son las potenciales amenazas de carácter legal, normativo y ético. Los riesgos pueden estar asociados a privacidad y protección de los datos, seguridad de la información, uso de las redes sociales, gestión de la propiedad intelectual, conflictos de intereses entre terceros, prevención de delitos, seguridad y salud del trabajo, código de ética y de conductas, protección al consumidor, ciberseguridad y privacidad, ambientales, seguridad del producto, comercio, importación y exportación, prácticas anticorrupción, entre otros. Se recomienda asignar un código a cada uno de los riesgos identificados y una breve descripción de los mismos.

Paso 4. Evaluación de los riesgos de “compliance”

La evaluación de riesgos involucra identificar y analizar los riesgos principales con el objetivo de determinar la forma en la que estos puedan ser manejados y en consecuencia facilitar el cumplimiento de la misión y visión de la organización. En este paso se asocian las posibles consecuencias, probabilidad de ocurrencia y dificultad de detección de los riesgos de cumplimiento de lo normado.

En esta investigación se propone para la evaluación del riesgo de cumplimiento normativo la ecuación (1). En el caso de las consecuencias del riesgo, los expertos emitirán sus valoraciones sobre la base de las dimensiones de la sostenibilidad enunciadas en el modelo de Triple Cuenta

de Resultados: económica, social y ambiental. Luego se selecciona para calcular el índice de criticidad la consecuencia máxima (C_{max}).

Paso 5. Elaboración del plan de acciones para el cumplimiento normativo

En este paso se elabora el plan las acciones para mitigar los riesgos del “compliance” en cada uno de los procesos de negocio promoviendo una cultura de cumplimiento en toda la organización. La comunicación del programa se realizará de manera periódica y sistemática hacia todos los niveles de la organización, siendo importante que todos los trabajadores conozcan sus obligaciones éticas y legales, especialmente las relacionadas con los procesos que ejecutan.

Luego de implementadas las acciones, se deben evaluar los riesgos de compliance definidos, para valorar el impacto de las acciones propuestas en la mitigación de los riesgos.

La aplicación del procedimiento en una entidad tecnológica permitió priorizar y tomar medidas para la mitigación de los riesgos de compliance; identificándose como los riesgos de mayor nivel de criticidad asociados al proceso de Gestión de los Recursos Humanos los siguientes: Accidentes o enfermedades profesionales de los trabajadores, inadecuado uso del acceso a internet, inadecuado levantamiento de necesidades de capacitación, elaboración deficiente de las pre Nóminas y el Inadecuado sistema de pago a trabajadores.

DISCUSIÓN

Al desarrollarse el proceso de gestión de riesgos en la organización en cuestión se identificó en la fase de preparación previa que la misma no tenía en cuenta las legislaciones vigentes para la identificación de los riesgos; lo cual conllevó a un análisis de la norma internacional ISO 19600 para aplicar el cumplimiento con lo normado al proceso en cuestión. Además, al desarrollar el proceso no se tenían en cuenta las consecuencias de los riesgos en las diferentes dimensiones de la sostenibilidad lo que imposibilitaba el análisis multidimensional de estos.

Para el cálculo de la cantidad, selección y formación de la comunidad de expertos, se propone seguir los procedimientos propuestos en las investigaciones de los autores (Michalus, Castro, William, & Hernández-Pérez, 2015; J. A. Plasencia-Soler, Marrero-Delgado, Nicado-García, & Aguilera-Sánchez, 2017).

Posteriormente, al desarrollar la evaluación de los riesgos se puede utilizar el Análisis de Modos de Fallas, Efectos y Criticidad (AMFEC) para calcular un índice de criticidad (IC) o índice de priorización de los riesgos (IPR) tal y como proponen los autores (Selvan, Jegadheesan., Varthanan, & Senthilkumar, 2013; Shanfeng Z, Mengwei L, Haiyan Z, & Ruili Z, 2015). En la

Tabla 2 se muestra las ecuaciones (2), (3), (4) empleadas por diferentes autores para la priorización de los riesgos.

Para la evaluación de los riesgos de cumplimiento normativo según las consecuencias, la probabilidad de ocurrencia y su detectabilidad, se propone utilizar una escala de evaluación tal y como proponen los autores (Franceschini & Galetto, 2001).

Esta evaluación debe integrarse a la evaluación de riesgos de la entidad por cada uno de los procesos definidos. Para la evaluación de los riesgos se propone utilizar una adaptación del formato propuesto por (Bolaño-Rodríguez Y., 2014) en su tesis doctoral. Este permitiría comparar el índice de criticidad de los riesgos evaluado en la fase inicial de la implantación del modelo con el valor del índice de criticidad residual de los riesgos luego de implantado el programa de acciones de cumplimiento normativo.

Tabla 2: Ecuaciones enunciadas para calcular la criticidad del riesgo

Autor	Ecuaciones
Castillo-Serpa A.M. et al., 2009; Selvan et al., 2013; Matotek & Regodic, 2015	$IPR = S * O * D \quad (2)$ <p>Donde: IPR: Índice de prioridad del riesgo O: Probabilidad de ocurrencia. S: Severidad del efecto potencial. D: Efectividad de detección para controlar el origen de la causa.</p>
Juan Antonio Plasencia-Soler, Marrero-Delgado, Nicado-Garcia, & Collada-Peña, 2016	$Ic = \frac{D}{Q * C} \quad (3)$ <p>Donde: Ic: Índice de criticidad del riesgo Q: Probabilidad de ocurrencia.</p>
Aguilar-Otero J. R., Magaña-Jiménez D, & Torres-Arcique R, 2010	$I_c = F * C_{max} \quad (4)$ <p>Donde: F: Frecuencia de ocurrencia del riesgo. Cmax: Consecuencia máxima según la dimensión en que impacte.</p>

Fuente: Elaboración propia.

El análisis de riesgos de compliance en las entidades de las tecnologías de la información y las comunicaciones es de vital importancia para el cumplimiento de los objetivos, por lo cual el procedimiento propuesto en este trabajo permitirá identificar los puntos en los que pueden fallar de contacto entre el marco legal, ético y normativo con las actividades asociadas a los procesos de la organización.

CONCLUSIONES

La incorporación de este procedimiento a la gestión de riesgos del cumplimiento ético y normativo permite a la organización, desde la gestión de riesgos, identificar las deficiencias de las actividades de los procesos de la organización, asociadas al cumplimiento legal, ético y normativo y permite mejorar los indicadores del desempeño organizacional.

REFERENCIAS BIBLIOGRÁFICAS

- Aguilar-Otero J. R., Magaña-Jiménez D, & Torres-Arcique R. (2010). Análisis de modos de falla, efectos y criticidad (AMFEC) para la planeación del mantenimiento empleando criterios de riesgo y confiabilidad. *Revista Tecnología Ciencia y Educación*, 25(1), 15-26.
- Bolaño-Rodríguez Y. (2014). *Modelo de dirección estratégica basado en la administración de riesgos para la integración del sistema de dirección de la empresa* (Tesis presentada en opción al grado científico de Doctor en Ciencias Técnicas). Universidad Tecnológica de la Habana José Antonio Echeverría, La Habana. Cuba.
- Castillo-Serpa A.M., Brito-Ballina M.L., & Fraga-Guerra E. (2009). Análisis de criticidad personalizados. *Ingeniería Mecánica*, 12(3), 1-12.
- Cordero Morales D., R. C. Y., & Torres Rubio Y. (2013). Sistema de Razonamiento Basado en Casos para la identificación de riesgos de software. *Revista Cubana de Ciencias Informáticas*, 7(2), 95-112.
- Díaz Concepción A, Pérez Rodríguez F, Del Castillo Serpa A, & Brito Vallina M. L. (2012). Propuesta de un modelo para el análisis de criticidad en plantas de productos biológicos. *Ingeniería Mecánica*, 15(1), 34-43.
- Franceschini, F., & Galetto, M. (2001). A new approach for evaluation of risk priorities of failure modes in FMEA. *International Journal of Production Research*, 39(13), 2991-3002. <http://doi.org/https://doi.org/10.1080/00207540110056162>
- Hernández Díaz N., Y. L. M., & Cuza García B. (2013). Modelos causales para la Gestión de Riesgos. *Revista Cubana de Ciencias Informáticas*, 7(4), 58-74.
- ISO. (2018). *ISO 31000:2018, Risk management – Guidelines, provides principles, framework and a process for managing risk*. Ginebra, Suiza: International Organization for Standardization.
- ISO-19600. (2014). *Compliance management systems -- Guidelines* (p. 28). Geneva, Switzerland: International Organization for Standardization.
- Martell-Fernández V., Z.-V. Y. (2014). Modelo para el análisis de riesgos en Líneas de Productos de Software. *Revista Cubana de Ciencias Informáticas*, 8(1), 82-98.

- Martínez, E. C. (2017). Ecu@Risk, Una metodología para la gestión de Riesgos aplicada a las MPYMEs. *Enfoque UTE*, 8(1), 107-121. <http://doi.org/10.29019/enfoqueute.v8n1.140>
- Matotek, M., & Regodic, D. (2015). HUMAN RESOURCE RISK MANAGEMENT IN SUPPLY CHAIN. *DYNA Management*, 3(1). Recuperado a partir de <https://www.dyna-management.com/search-content-2/human-resource-risk-management-in-supply-chain>
- Michalus, J. C., Castro, S., William, A., & Hernández-Pérez, G. (2015). Método de expertos para la evaluación ex-ante de una solución organizativa. *Visión de futuro*, 19(1), 0-0.
- NC-ISO 9001. (2015). Sistemas de gestión de la calidad — Requisitos. Oficina Nacional de Normalización. Recuperado a partir de <https://www.iso.org/obp/ui/#iso:std:iso:9001:ed-5:v1:es>
- Pérez Moya O., Z. V. Y. (2013). Proceso para gestionar riesgos en proyectos de desarrollo de software. *Revista Cubana de Ciencias Informáticas*, 7(2), 67-82.
- Plasencia-Soler. (2018). *Modelo para contribuir a la sostenibilidad de entidades de las tecnologías de la información y las comunicaciones desde la gestión estratégica* (Doctoral). UCI, La Habana, Cuba.
- Plasencia-Soler, J. A., Marrero-Delgado, F., Nicado-García, M., & Aguilera-Sánchez, Y. (2017). Procedimiento para la priorización de Factores Críticos de Éxito. *DYNA*, 84(202), 26-34. <http://doi.org/10.15446/dyna.v84n202.62084>
- Plasencia-Soler, J. A., Marrero-Delgado, F., Nicado-Garcia, M., & Collada-Peña, I. (2016). Evaluación de la sostenibilidad de organizaciones cubanas. *DYNA MANAGEMENT*, 4(3). <http://doi.org/10.6036/mn7966>
- Sablich Huamani C.A. (2010). *Aplicación de un Modelo de Dirección Estratégica en Época de Crisis, estudio de caso: Agroexportadora de Perú* (Proyecto final para optar por el título de Máster en Dirección Estratégica). Universidad de Lima, Perú.
- Segura Pinzón J.C. (2011). *Modelo de Administración de Riesgos aplicado en el análisis del aseguramiento de ingresos en compañías de telecomunicaciones bajo el marco de una administración por objetivos* (Tesis para optar por el título de máster en Administración). Universidad Nacional de Colombia. Facultad de Ciencias Económicas, Bogotá, Colombia.
- Selvan, T. A., Jegadheesan., C., Varthanan, P. A., & Senthilkumar, K. M. (2013). A Novel FMEA approach for ranking Mould Designs in foundries. *Life Science Journal*, 10(2), 51-60.
- Shanfeng Z, Mengwei L, Haiyan Z, & Ruili Z. (2015). Aircraft Fuel System Fuzzy FMEA and FMECA Analysis. Presentado en International Conference on Information Sciences, Machinery, Materials and Energy (ICISMME 2015), Chongqing, China.

- Subburaman, K. (2010). *A Modified FMEA Approach to Enhance Reliability of Lean Systems* (Master's Thesis). University of Tennessee, Knoxville, Tennessee. Recuperado a partir de http://trace.tennessee.edu/utk_gradthes/664
- Vargas Aguila, Y., Aguila, Y. V., Perez, J. C. A., Rodríguez, A. M. G., & Fumero, D. M. S. (2017). Sistema Integral de Control Interno para el Vicedecanato de Administración y Servicios de la Facultad 3. *Serie Científica de la Universidad de las Ciencias Informáticas*, 10(2), 37-51.

Datos de los autores

- Yasmany Aguilera Sánchez: *Ingeniero en Ciencias Informáticas, Profesor instructor, Universidad de las Ciencias Informáticas, La Habana, Cuba.* yasmanyas@uci.cu.
- Juan Antonio Plasencia Soler: *Doctor en Ciencias, Profesor Auxiliar, Universidad de las Ciencias Informáticas, La Habana, Cuba* juanps@uci.cu.
- Fernando Marrero Delgado: *Doctor en Ciencias, Profesor Titular, Universidad Central de Las Villas "Martha Abreu de las Villas", Las Villas, Cuba.* fmarrero@uclv.edu.cu.