Evaluación de los riesgos de cumplimiento normativo

Evaluation of compliance risks

Ing. Yasmany Aguilera Sánchez [1]

M.Sc. Juan Antonio Plasencia Soler [2]

Dr. C. Miriam Nicado García [3]

M.Sc. Mailín Ochoa Calzadilla [4]

[1]Dir. Recursos Humanos, Universidad de las Ciencias Informáticas. Cuba.

[2] Facultad 4, Universidad de las Ciencias Informáticas. Cuba.

[3] Facultad 1, Universidad de las Ciencias Informáticas. Cuba.

[4]Recursos Humanos, Universidad de las Ciencias Informáticas. Cuba.

Resumen

Las organizaciones se encuentran en constante búsqueda de nuevas estrategias de trabajo que le permitan ser más competitivas a través de la utilización de nuevas herramientas científicas y tecnológicas. La gestión de riesgos de cumplimiento normativo es una de las herramientas actuales utilizadas por la gerencia para asegurar el cumplimiento de los objetivos trazados y mantener la sostenibilidad de la organización. El presente trabajo propone un procedimiento para la gestión de los riesgos de cumplimiento normativo en una organización basados en la norma internacional 19600 para la gestión de riesgos de cumplimiento de la Organización Internacional de Normalización y los índices de criticidad propuestos por diversas investigaciones en la temática. Los resultados de la aplicación del procedimiento son expuestos a través de la elaboración de un mapa de riesgos residuales luego de implementada la propuesta en una organización cubana.

Palabras clave: programa de ética y compliance; gestión de riesgos; índice de criticidad

Abstract

The companies are constantly searching new work strategies for achievement more competitive through the use of new scientific and technological tools. The compliance risk management is one of the current tools used by manager to ensure the success of the objectives maintaining the sustainability. The present research proposes a procedure for the compliance risks management in an organization based on the international standard 19600 for the compliance risk management of the International Organization for Standardization and the criticality indexes. The results of the application of the procedure are exposed through the elaboration of a map of residual risks after implementing the proposal in a Cuban organization.

Keywords: *ethics and compliance program; risk management; criticality index*

Introducción

La correcta identificación y evaluación de los riesgos se está convirtiendo en un elemento crucial en la gestión de las organizaciones. En un entorno cada vez más cambiante por el vertiginoso avance de las ciencias y las tecnologías, lograr anticiparse a situaciones potencialmente hostiles, supone una ventaja competitiva que contribuye de forma sustancial a lograr los objetivos estratégicos en las organizaciones (Guevara et al., 2018).

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 (Sablich Huamani C.A, 2010; Segura Pinzón J.C, 2011; 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.

En años recientes, varios investigadores proponen llevar a cabo los programas de cumplimiento normativo mediante la gestión de riesgos de compliance, lo que ha permitido integrar dos poderosas herramientas de gestión para el logro de la sostenibilidad organizacional.

El presente trabajo tiene como objetivo desarrollar una metodología para la evaluación de riesgos de cumplimiento normativo. Para el cumplimiento de este objetivo se desarrolló un estudio la norma internacional ISO 19600, así como los índices de criticidad propuestos por prestigiosos académicos internacionales. La investigación se estructura de la siguiente forma: un primer apartado donde se exponen los fundamentos de la metodología; un segundo apartado donde se muestran los principales resultados de la aplicación de la propuesta en una organización cubana y; finalmente se exponen las conclusiones del estudio.

Metodología

Teniendo 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, se propone una metodología para la evaluación del cumplimiento normativo en una organización. La metodología sigue un ciclo de Deming o ciclo PHCA (Planear, Hacer, Controlar, Actuar) para desarrollar cada una de sus etapas tal y como muestra la Figura 1.

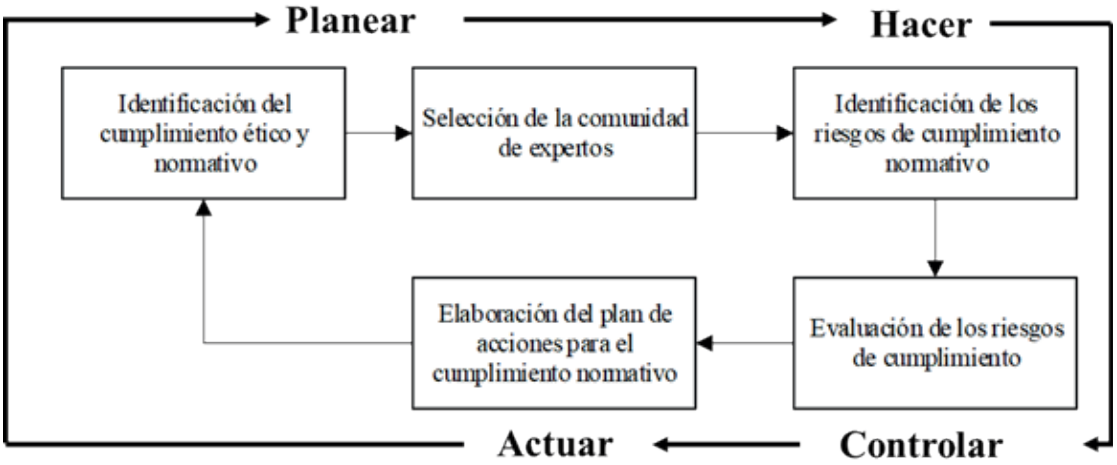

Figura 1 Metodología para el diseño de un programa de ética y "compliance".

Fuente: Elaboración de los autores basado en la (Contraloría General de la República, 2011; ISO-19600, 2014)

Paso 1. Identificación del cumplimiento ético y normativo

En este paso se identifican y documentan 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 continúo.

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.

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; Sarache-Castro, Costa-Salas, & Martínez-Giraldo, 2015).

Paso 3. Identificación de los riesgos de cumplimiento normativo

En este paso se identifican los riesgos asociados con el cumplimiento de lo normado. Estas son las potenciales amenazas de carácter legal, normativo y ético. Los riesgos de "compliance" pueden estar asociados 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, practicas 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.

Para este paso 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 (Castillo-Serpa A.M., Brito-Ballina M.L., & Fraga-Guerra E, 2009; Subburaman, 2010; Díaz-Concepción A, Pérez-Rodriguez F, Del Castillo-Serpa A, & Brito-Vallina M. L, 2012; Selvan, Jegadheesan., Varthanan, & Senthilkumar, 2013; Shanfeng Z, Mengwei L, Haiyan Z, & Ruili Z, 2015). En la Tabla 1 se muestra las ecuaciones (1), (2), (3), (4) empleadas por diferentes autores para la priorización de los riesgos.

Tabla 1 Ecuaciones enunciadas para calcular la criticidad del riesgo.

Autor	Ecuaciones
(Castillo-Serpa A.M. et al., 2009; Selvan et al., 2013; Matotek & Regodic, 2015)	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.
(Subburaman, 2010)	Donde: VER: Valor Evaluado del Riesgo
(Juan Antonio Plasencia-Soler, Marrero-Delgado, Nicado-Garcia, & Collada-Peña, 2016)	Donde: Ic: Índice de criticidad del riesgo Q: Probabilidad de ocurrencia.
(Aguilar-Otero J. R., Magaña-Jiménez D, & Torres-Arcique R, 2010)	Donde: F: Frecuencia de ocurrencia del riesgo. Cmax: Consecuencia máxima según la dimensión en que impacte.

Fuente 1 Elaboración propia a partir de las fuentes citadas.

Los autores de la presente ponencia teniendo en cuenta los estudios anteriores, proponen para la evaluación del riesgo de cumplimiento normativo la ecuación (5). 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 (*Cmax*).

$I_c = F^{*}Cmax^{*}D$

Dónde:

I_c: Índice de criticidad.

F: Frecuencia de ocurrencia del riesgo.

Cmax: Valor máximo de las consecuencias según las dimensiones de la sostenibilidad.

D: Detección.

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).

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. 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.

Resultados y discusión

El procedimiento descrito anteriormente se aplicó al proceso de Gestión de los Recursos Humanos en una organización de las Tecnologías de la Información. Primeramente, la dirección de la organización identificó el marco legal, ético y normativo asociado al proceso seleccionado. Seguidamente se seleccionaron y capacitaron los siete expertos que realizarían la definición y evaluación de los riesgos. Luego los expertos identificaron cada uno de los riesgos del proceso de recursos humanos de la organización, tal y como se muestra en la Tabla 3.

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 prenóminas
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 Protección a la Maternidad de la mujer trabajadora	Modificaciones de períodos de maternidad

R08	Res 283/2009 Ley de Seguridad Social	Inadecuado cálculo de años de servicio de un trabajador para la jubilación
R09	Código de Ética	Inadecuado uso del acceso a internet
R10	NC 18000, 18001, 18002/ 2005 Sistema de gestión de Seguridad y Salud en el trabajo	Accidentes o enfermedades profesionales de los trabajadores
R11	Res 85/2016 Reglamento Para la aplicación de las Categorías Docentes de la educación superior	Entrega de certificado de categoría docente erróneamente
R12	Res 43/2012 Regulaciones laborales aplicables a los trabajadores que solicitan viajar al exterior por asuntos particulares	Desconocimiento por parte del jefe de los verdaderos motivos de ausencia de un trabajador
R13	Res 9/2016 Organización salarial del sistema de la educación superior	Inadecuado sistema de pago a trabajadores
R14	Res 95/2017 La atención al hombre. El mejoramiento de las condiciones de trabajo y el Sistema de incentivos y premios	Inadecuada entrega de estimulación

Los riesgos identificados fueron evaluados por la comunidad de expertos mediante por consenso. Luego fue calculado el Índice de Criticidad (Ic) de los riesgos a través de la ecuación (5). La Figura 2 muestra el mapa de riesgos de cumplimiento normativo teniendo en cuenta las consecuencias y la probabilidad de ocurrencia.

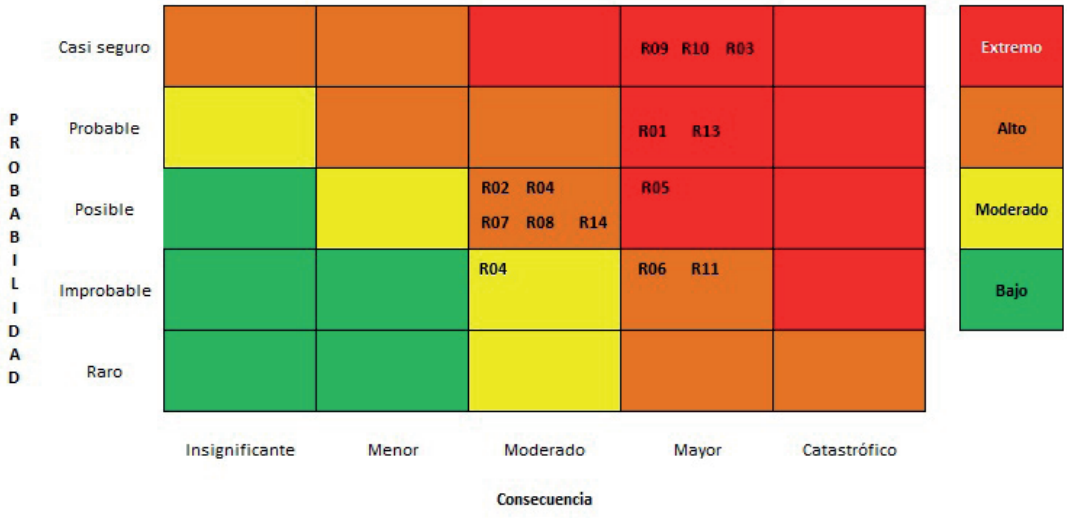

Figura 2 Mapa de riesgos residuales.

De acuerdo a la priorización de los riesgos fueron implementados acciones de control para reducir sus impactos en la organización. La Figura 3 muestra la variación del índice de criticidad luego de aplicadas las medidas para su mitigación o el índice residual de los riesgos fundamentales.

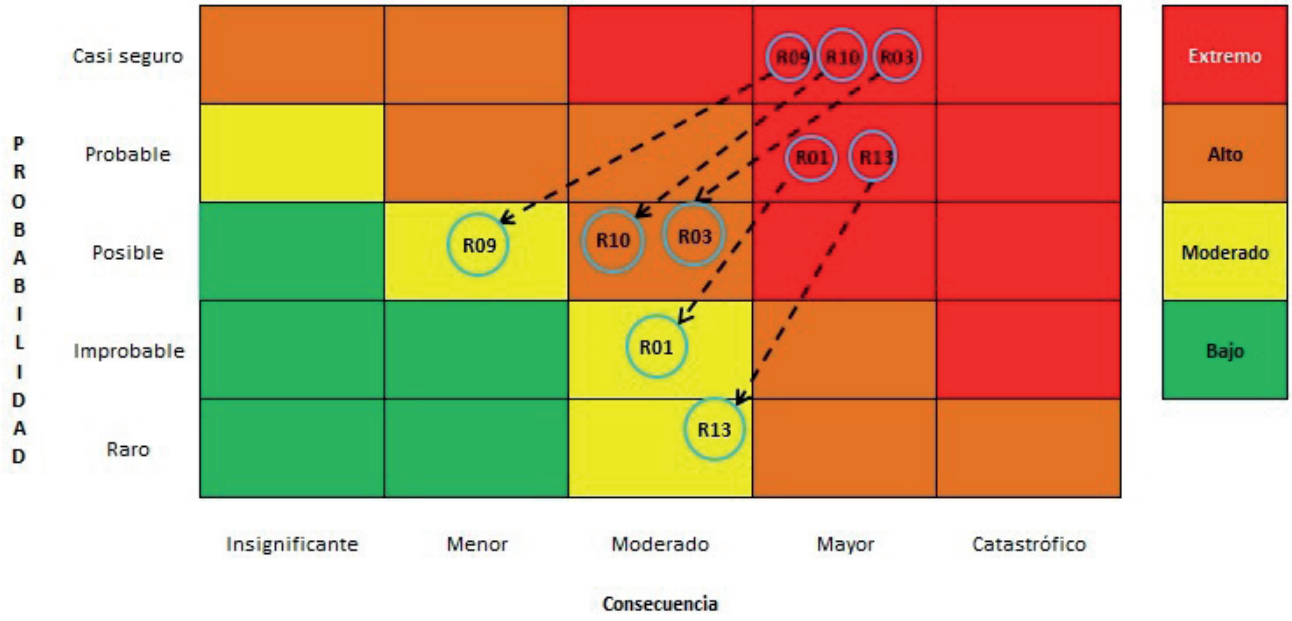

Figura 3 Mapa de riesgos residuales.

Conclusiones

La incorporación a la gestión de riesgos de la gestión del cumplimiento ético y normativo posibilita a la organización identificar, evaluar, mitigar y monitorear desde la gestión de riesgos, las deficiencias de las actividades de los procesos de la organización asociadas al cumplimiento legal, ético y normativo, permitiendo una mayor eficiencia en el cumplimiento de los objetivos.

El procedimiento propuesto permite integrar el estándar internacional ISO 19600 con los análisis de criticidad para la gestión de riesgos fundamentados en la literatura científica internacional; facilitando mejoras prácticas a través del cumplimiento de los pasos descritos, lo cual permite la mejora continua de la mitigación de los riesgos la utilizar el ciclo Planear, Hacer, Controlar y Actuar.

La aplicación del procedimiento en una entidad tecnológica permite 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 prenóminas y el Inadecuado sistema de pago a trabajadores.

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, lo cual 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.

Referencias

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.

Contraloría General de la República. (2011). Resolución 60. Normas del Control Interno (Gaceta Oficial de la República, Vol. 109).

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-Rodriguez 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. https://doi.org/https://doi.org/10.1080/00207540110056162

Guevara, A., M, E., Feal Cuevas, N., Torres Torres, B., Echazábal Leal, A., & Lorenzo Roche, L. (2018). Propuesta metodológica para la gestión de riesgo en las organizaciones. Presentado en IV Evento Nacional de EXPERIENCIAS EN SISTEMAS INTEGRADOS DE GESTIÓN. Recuperado a partir de http://dspace.uclv.edu.cu:8089/xmlui/handle/123456789/9412

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. https://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-con-

tent-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.

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, 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. https://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). https://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.

Sarache-Castro, W. A., Costa-Salas, Y. J., & Martínez-Giraldo, J. P. (2015). Environmental performance evaluation under a green supply chain approach. DYNA, 82(189), 207-215.

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.