Article

Procedure for Integrated Risk Management at the University of Computer Sciences

Procedimiento para la gestión integrada de riesgos en la Universidad de las Ciencias Informáticas

Juan Fuentes Bauta[1*] http://orcid.org/0000-0003-0095-2047
Dr. Yuniel Bolaño Rodríguez[2] http://orcid.org/0000-0001-9391-2516

[1]University of Computer Sciences, Havana, Cuba
[2]Jose Antonio Echeverria, Technological University of Havana, Cuba

[*]Corresponding author: jbauta@uci.cu

ABSTRACT

Aim: To design a procedure for integrated risk management at the University of Computer Sciences, in Havana, Cuba, in order to strengthen internal control.

Methods: analytical-synthetic, system approach, and descriptive statistics.

Main results: the novelty of this procedure is the manner of risk identification, analysis, and quantification that might take place in every process and event, and have a negative impact on objective fulfilment. Another important result is the protection of resources, and the observance of laws and regulations, in order to meet the strategic and work objectives. The determination of the control objectives and their plan of prevention was also innovating. **Conclusions**: the outcome from the partial application of the procedure in the Managing Office for Internal Control at the university concluded with the identification of 15 risks and 48 related causes. Four of the risks were moderate, seven were low, and two were trivial. Six of them were considered relevant, and underwent integrated analysis that led to five control objectives and twelve actions.

Key words: integrated risk management; processes; internal control; control objectives.

RESUMEN

Objetivo: Un procedimiento para la gestión integrada de riesgos en la Universidad de las Ciencias Informáticas, La Habana, Cuba, como parte del fortalecimiento del sistema de control interno.

Métodos: analítico-sintético, enfoque de sistema y estadística descriptiva.

Principales resultados: el procedimiento se distingue por la forma de identificación, análisis y cuantificación de los riesgos que pueden ocurrir en cada uno de los procesos y sus actividades, y que impactan negativamente en el cumplimiento de los objetivos, la protección de los recursos y el cumplimiento del marco legal y regulatorio, para poder alcanzar los objetivos estratégicos y de trabajo. Se distingue también la determinación de los objetivos de control y su plan de prevención.

Conclusiones: se muestran los resultados de la aplicación parcial del procedimiento en la Dirección de Control Interno del centro; se identificaron 15 riesgos y 48 causas asociadas a estos. Del análisis, los riesgos determinados fueron: cuatro moderados, siete bajos y dos triviales, de los cuales se establecieron seis riesgos relevantes, a los que se les realizó un análisis integrado para determinar cinco objetivos de control y 12 acciones.

Palabras clave: gestión integrada de riesgos; procesos; control interno; objetivos de control.

Received: 25/04/2019

Accepted:13/02/2020

INTRODUCTION

Nowadays, universities must face several risks, due to the multiplicity of daily events held in any given location (national, international, regional, and local), which could be

dynamic and uncertain. Hence, it is necessary to improve management models (Almuiñas and Galarza, 2016a,b).

In order to improve organizational performance, a system that exerts internal control inherent to all processes, activities, and operations conducted in higher education institutions, should be implemented. This system should have a preventive approach that permits previous identification of events or adverse effects, which might have a negative impact on goal fulfillment, the utilization or resources and their yields, as well as compliance of the legal and regulatory frames. To conduct such preventive approach, and contribute to improvements in the levels of efficacy and efficiency, it is necessary to implement a risk management process, that allows for identification, analysis, evaluation, and treatment of the main risks affecting the performance and function of the Internal control system (Mendoza, Bolaño, and Mendoza, 2017).

In that sense, the Internal Control Office (DCI), linked to the First Deputy-Rectorate Office, is the one in charge of providing methodological assistance to internal control management at the University of Computer Sciences (UCI), which is materialized in all the organizational units of the institution. Its mission is to evaluate, provide advisory, and supervise the implementation of the internal control system, with a committed staff, whose principles and ethical values ensure reasonable safety in University processes, enabling efficient use and control of earmarked resources, under the current regulations and legislation.

Control actions conducted by DCI showed the existence of problems in the determination of control goals based on the main risks. Additionally, the information in relation to the prevention plan, and adequate risk management, either due to little specialization training of staff engaged in the application of risk management activities or the poor culture in this topic, which limit the scope of analysis at any level, in the institution. These are indispensable requisites to accomplish those goals, protect their resources, and comply with the regulatory and legal frames.

Therefore, the aim of this paper was to design a procedure for integrated risk management at UCI, as part of strengthening actions of the internal control system (SCI), considering the changes of scenarios, and research done in risk management. Accordingly, cadres and specialists can acquire the skills to implement the risk

prevention and management components, in Resolution 60/11, from the Comptroller General of the Republic (CGR), providing a tool for risk management of processes, and activities that can affect the compliance of objectives and goals set in every area of work. In that direction, a review of the literature and documents was performed, together with the analysis of the outcome of research and interviews.

DEVELOPMENT

A rationale for integrated risk management

Organizations advance toward an integrated-approach control frame, covering the entire payroll; it is based on a series of tools to achieve effective internal control within a work philosophy centered on continuous improvement, through strategy definitions (Alfonso, 2007; Bolaño, 2014; Comptroller General of the Republic of Cuba [CGR], 2011). Integrated risk management is comprised in that frame, which consists in timely detection of diverse risks that can affect the organization to generate anticipating strategies, in order to turn them into opportunities that contribute to operational efficacy and efficiency, and help accomplish the mission and vision, in compliance with the legislation and standards established.

This integrated risk management involves an analysis of the internal and external contexts of the organization, and requires proper internal control. In Cuba, CGR Resolution No. 60/2011, on the Standards of the Internal Control System aims to reach results in efficiency, order, and discipline. Accordingly, it is important to foster a culture of control, and encourage awareness on its relevance.

CGR (2011) defines internal control as a process integrated to operations with a continuous improvement approach applied to all activities pertaining to management, which are performed by the board of directors and other staff members. Besides, it is implemented through integrated systems of standards and procedures that contribute to foresee and limit internal and external risks, while providing reasonable safety in terms of meeting institutional objectives, and adequate accountabilities.

Another component describes risk management and prevention for SCI, declaring that the Risk Prevention Plan (RPP) is a work tool management to provide systematic follow up of certain control objectives. It is updated and examined periodically by workers who present facts when required (CGR, 2011).

Therefore, the internal control system should be a space of integration of all the risks of an organization. Thus, risk management can be understood as an interative process that stems from organizational policies. With the utilization of every existing resource and technology, the organization performs a set of activities such as, risk identification, analysis, and evaluation; decision-making based on cost/benefit, whose actions are intended to stop, eliminate, reduce, and control the adverse effects (risks) realized in the organizational processes, affecting the performance of organizations(Bolaño, 2014)

Theoretical and practical risk management studies (Bolaño, 2014; Bolaño, Alfonso, Pérez, and Arias, 2014; Mendoza *et al*., 2017; Rodríguez, Fernández, and de Dios, 2015; Varela, Oquendo, Romero, and Zúñiga, 2019) emphasize on the fact that the application of integrated risk approach will enable anticipation in decision-making with systemic, strategic, and participatory approaches.

Procedure for Risk Management at the University of Computer Sciences

All the staff members from every area will conduct identification, analysis, and evaluation of the risks that can affect the fulfillment of objectives and goals, associating them to the causes and conditions, and the control objectives. Then the risks included in the prevention plan will be determined.

Below are different rationales of the procedure for integrated risk management, as part of a strengthening process of the system of internal control. It is made of different theoretical elements developed by Bolaño (2014), in the PhD thesis, along with the SCI standards presented in Resolution 60/2011 from CGR.

Key concepts:

Process: A set of interrelated or interacting activities that change input elements into output elements (good/service). (Technical Committee ISO/TC 176, 2015).

Risk Likelihood of occurrence of undesired events in the processes of the organization, which produce negative impacts. (Bolaño, 2014)

Causes of risk: These elements lead to the occurrence of a risk. The causes of risks can be, situations, phenomena, omissions, violations of set rules, decisions, external and internal factors, events, and unexpected changes (Bolaño, 2014).

Control objectives: they are the result or purpose desired with the application of control procedures, which should verify the risks identified, and depend on the policy and strategy of the organization (CGR, 2011).

The procedure for integrated risk management at UCI, as part of strengthening the internal control system is performed in six steps, as shown in Fig.1.

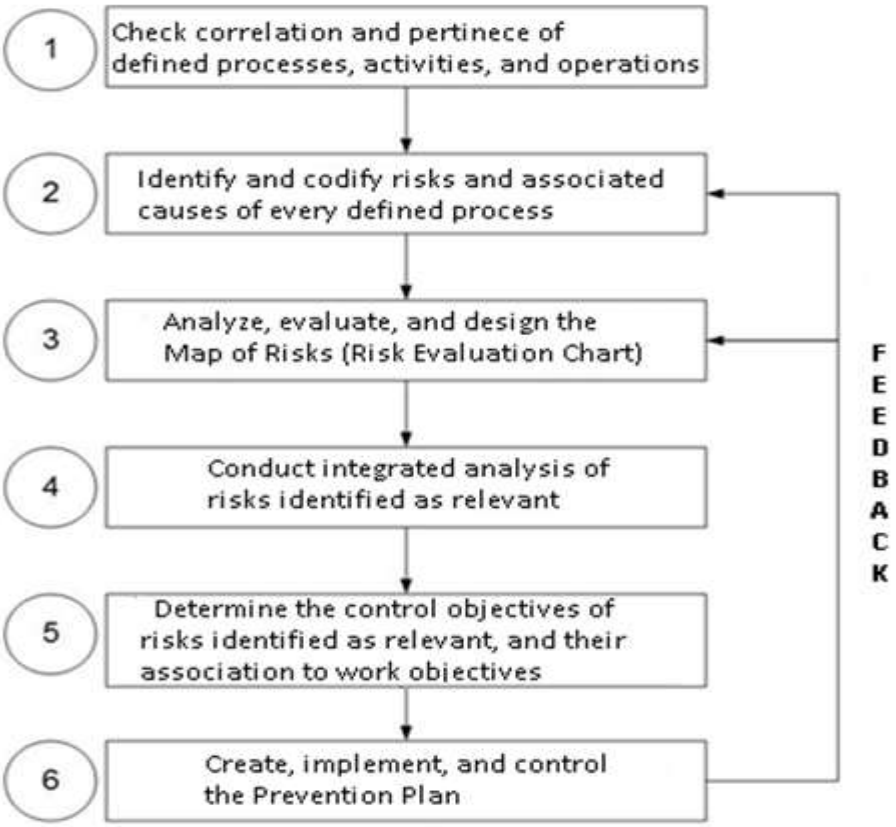

Fig.1. Procedure for integrated risk management

Source: Self-made.

Step 1. To review the correlation and pertinence of defined processes, activities, and operations.

Every activity performed by the entity should be included in its processes, thus acknowledging process approach to understand the way the organization functions, which includes activities and operations. The processes that take place in the organization, regardless of their management or not. The absence of management will probably affect their efficacy and efficiency, and therefore, their strategic goals. Identifying, analyzing, managing, and improving processes would be more effective instead (Alfonso, 2007).

This step requires a review of all processes defined by the entity or area, to determine the activities of all the processes identified, and to verify the activities and operations that influence on the fulfillment of the entity's or facility's goals.

Step 2: To identify and codify risks and associated causes of every process defined.

The risks and their causes are identified in every process. The following question can be used to identify their risks: What can occur in previously identified processes P1, P2, Pn that might affect the performance of an entity or area?

Upon identifying the risk, assessment of possible negative impacts on goal accomplishment, protection of resources, the environment, the compliance of legislation and standards governing the entity, the ethical behavior of staff and executives in the organization, should be performed. A code must be assigned to the risks identified. For instance, risk No. R0301 is risk number one from process number three. To identify the risks, the organization may consider a group of elements and criteria, accordingly, which are shown below:

- ✓ The causes and conditions of illegal behavior, criminal acts, as well as flaws detected by internal or external control actions.
- ✓ Complaint and reports filed.
- ✓ Weaknesses, threats, strengths, and opportunities (SWOT).
- ✓ Analysis of failure to comply with the work balance.
- ✓ Processes: process sheet, interrelation, and output variables.
- ✓ List of previously identified risks at the entity or facility, and the ones defined in the Competence Profile model of work posts.

- ✓ Resources of the entity or facility (humans, material, technological, financial, informational).
- ✓ Legislation, standards, or resolutions that must be observed.

They must take into account risk identification: plans and/or information safety, labor security and health, and security and protection.

They must be taken into account to identify risks:

- ✓ Within the same process, a risk cannot be the cause of another direct risk.
- ✓ A process's risk cannot be the cause of another process's risk.
- ✓ A risk can be identified in a process in which such process is not responsible for the occurrence of the risk itself.

The external and internal causes of each previously identified risk are identified. Acknowledging the causes and gathering opinions from all the staff involved in process activities and operations is important. Accountability meetings and other spaces to hold discussions with the staff are necessary. The causes should be codified as well; for instance, Cause C030102 is cause No. 2 of risk No. 1, which had been identified in process No. 3.

Step 3: To analyze, evaluate, and design the risk map (risk evaluation table) (Table 5).

Upon identification, risks are measured depending on the estimated occurrence or impact. Risk analysis is a cognitive process in which, based on the information available, the likelihood of occurrence of certain events is determined, along with the extent of their consequences and impacts, in order to provide data to be used in their evaluation and treatment (Albanese, 2012; Bolaño, 2014; Palma, 2011; Sulca and Becerra, 2017; Torres, Malta, Zapata, and Aburto, 2015).

To estimate the likelihood of risk occurrence:

The estimation of likelihood is estimated from the geometric mean between the values of the incidence level (il) of risk causes upon occurrence, and the level of control lack (cl) on the risk causes. It can be expressed through the following equation:

$$P = \sqrt[2]{il * cl} \quad \text{Where} \qquad 0 \leq il \leq 1 \qquad 0 \leq nd \leq 1$$

The il and cl values can be obtained from the descriptions in Tables 1 and 2.

Table 1: Determination of the incidence level of risk causes upon risk occurrence

Description of the incidence level of risk upon risk occurrence.	Evaluation
The risk causes or factors have full incidence and power on risk occurrence.	1.0
The risk causes or factors have an almost total incidence and high power upon risk occurrence.	0.9
The risk causes or factors have high incidence and power upon risk occurrence.	0.8
The risk causes or factors have a high incidence and almost high power upon risk occurrence.	0.7
The risk causes or factors have mid incidence and slightly higher power than moderate risk occurrence.	0.6
The risk causes or factors have mid incidence and moderate power upon risk occurrence.	0.5
The risk causes or factors have an almost mid incidence and slightly lower power than moderate upon risk occurrence.	0.4
The risk causes or factors have an almost mid incidence and low power upon risk occurrence.	0.3
The risk causes or factors have little incidence and low power upon risk occurrence.	0.2
The risk causes or factors have almost no incidence and very low power upon risk occurrence.	0.1
The risk causes or factors have no incidence (no risk).	0.0

Source: (Bolaño, 2014)

Table 2 Determination of lack of control of risks causes

Description of control lack of risk causes or factors	Evaluation:
Risk causes or factors are out of control.	1.0
Risk causes or factors are almost out of control.	0.9
Risk causes or factors are little controlled, with very low effectiveness upon risk occurrence.	0.8
The risk causes or factors are little controlled, with low effectiveness upon risk occurrence.	0.7
The risk causes or factors are mid controlled, with low effectiveness upon risk occurrence.	0.6
The risk causes or factors are mid controlled, with intermediate effectiveness upon risk occurrence.	0.5
The risk causes or factors are mid controlled, with slightly higher effectiveness than intermediate.	0.4
The risk causes or factors are quite controlled, with almost high effectiveness upon risk occurrence.	0.3
The risk causes or factors are quite controlled, with high effectiveness upon risk occurrence.	0.2
Risk causes or factors are almost completely controlled, with very high effectiveness.	0.1
Risk causes are completely controlled, with excellent effectiveness, with no risk occurrence (no risk).	0.0

Source: (Bolaño, 2014)

Information to estimate impact is shown in Table 3.

Table 3 Impact estimation

Category	Description	Evaluation
Catastrophic	Highly severe damage in process performance	10 9

Very high	Very significant damage in process performance	8 7
High	Significant damage in process performance	6 5
Mid	Moderate impact on the process	4 3
Low	Minimum impact on process performance	2 1
No impact	No impact on process performance	0

Source: Self-made

Risk value (VaR) is calculated to evaluate risk priority level (RPL), using the probability variables for risk occurrence (0 < P < 1), and the estimated impact (I), through this expression:

$$VaR = P * I$$

Where:

VaR = Risk value (points).

P = Risk estimated probability (0 < P < 1).

I = risk estimated impact (points).

When the risk value is calculated, it is located within the risk value range, as shown in Table 4, and the RPL is determined.

Table 4 Risk priority level

Risk value range	**Risk priority level (RPL)**	**Remarks**
VaR ≥ 6.4	Extreme	Must appear in the prevention plan.
3.6 ≤ VaR < 6.4	High	
1.5 ≤ VaR < 3.6	Moderate	To evaluate whether the facility has a prevention plan or not.
0.6 ≤ VaR < 1.5	Low	Implementing long-term actions that reduce or eliminate the risk. The risk map exists, but it is not included in the prevention plan.
VaR < 0.6	Trivial	The risk map exists, but it is not included in the prevention plan.

Source: Self-made.

Then, the risk map is designed (Risk Evaluation Chart), containing the data obtained, as shown in table 5.

Table 5 Risk map (Risk Evaluation Chart)

Process	Risks		Causes		Analysis			RPL
	Code	Description	Code	Description	P	I	VaR	

Source: Self-made

Whenever possible, any affectation or losses should be quantified through estimated assessment.

Step 4: To conduct integrated analysis of risks identified as relevant.

In this step, the main risks of the entity or facility are determined prior to integrated analysis, based on established cause-effect relationships. Therefore, it is necessary to analyze common causes, and if a process's risk is the cause of another risk identified in another process, or vice versa. The logical relations established between risks, depending on the relations of activities that generate the risks should also be analyzed.

The matrix of risk relations can be used to represent the cause-effect relations in an entity or facility (see Table 6). The example helps determine that a hypothetical critical situation occurs when there is no effective reduction of risk causes, and their risk-associated occurrence and impact will be stronger.

Table 6 Example of relationship matrix between the main risks

	Risk 1	Risk 2	Risk n	Total of causes
Risk 1				
Risk 2				
Risk n				
Total of effects				

Source: Modification of (Bolaño, 2014)

The risks evaluated as extreme, high, or moderate (up to 50% of total risks), are eligible to become major risks, and are elements to be considered in the control objectives of the entity or facility.

Step 5: To determine the control objectives of risks identified as relevant, and their association to the work objectives.

Each facility must design control objectives to minimize risks identified as relevant, and link them to the work objectives to achieve efficiency, efficacy, resource control, and compliance with the regulations. The control objective is generated and declared, depending on the negative version of the threat, turning it into a positive version of desire. In other words, analyzing what may be done inappropriately, and what can be suggested to avoid it.

Step 6: To assemble, implement, and control the prevention plan.

The prevention plan is designed according to the control objectives, in step 6, the last step (Table 7), whose actions are directed to the completion of control objectives, which, in turn, focuse on the reduction of relevant risks and their relations. This step also comprises the implementation of such plan, which requires leadership and motivation of executives and staff. During the implementation of prevention actions, other unexpected risks can originate, or the probability and impact variables can change. Hence, this procedure has a feedback from steps 2 and 3.

Table 7 Prevention plan proposal

Process	Control objectives	Risks		Causes		Actions	Responsible part	Implementing part	Deadline
		Code	Description	Code	Description				

Source: Self-made

The prevention plan consolidated at the deputy-rectorate offices, general director's offices, faculties, and directors with subordinates areas is no the sum of risks defined in the prevention plans of their subordinated areas, but the result of analysis of risks threatening the fulfillment of their goals and mission. Likewise, the consolidated plan will

be confirmed at university level, which will be reviewed and approved by the corresponding entity.

Results

The procedure was applied at the Science and Research Office, University of Computer Sciences. Each step of the procedure led to the following results:

In step 1, seven processes were identified (two were critical, and five were functional); in step 2, 15 risks and 48 associated causes were identified, with human resources management, being the process with the largest number of risks identified (six, and twenty causes), followed by internal control and continuous improvement processes, with four risks and eight causes (Fig. 2).

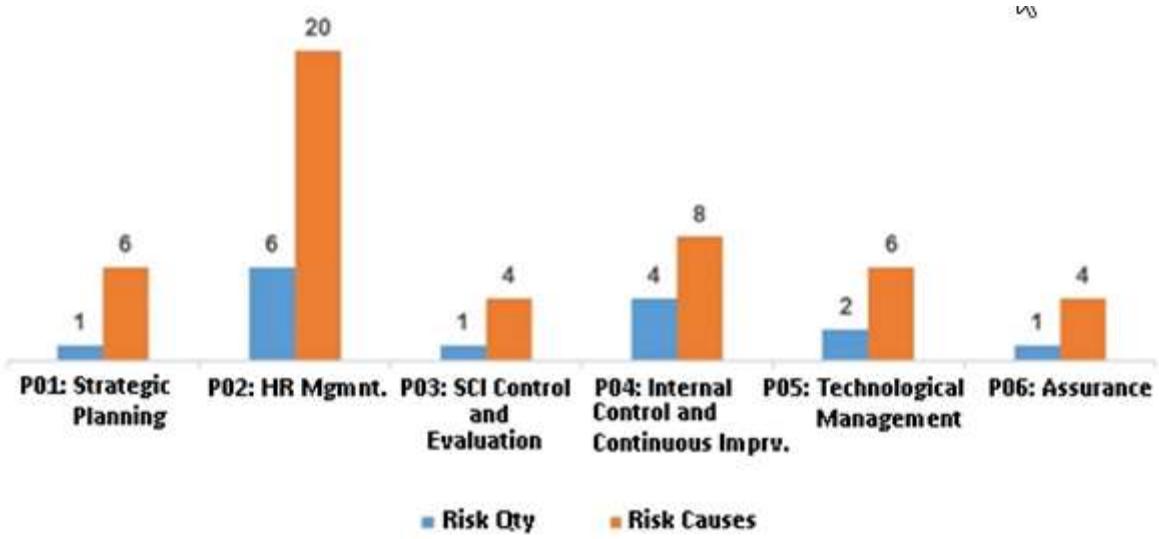

Fig 2 Risk identification by process

Source: Self-made

In step 3, every previously identified risk was analyzed; probability and estimated impact were evaluated, along with risk value, and their priority levels. As a result, two high, four moderate, seven low, and two trivial risks, were obtained.

Together with the major risks (Table 8), accounting for 40% of identified risks, step four was performed through integrated analysis, where attention was more centered on the

set of risks than on each risk separately. The cause-effect relations between these risks were determined with the relations matrix. This is shown in Table 9.

Table 8 Major risks

Process	Risks	
	Code	Description
P01: Strategic planning	R0101	Lack of compliance of work objectives
P02: Management of human resources	R0201	Loss of personal moral integrity
	R0204	Labor fluctuations
	R0206	Affectation to the health of staff
P03: Control and evaluation of the control system implemented in the university	R0301	Diffusion of unreliable information.
P04: Internal Control and continuous improvement	R0403	Loss of relevant documents

Source: Self-made.

Table 9 Relations matrix of major risks

	R0101	R0201	R0204	R0206	R0301	R0403	Total of causes
R0101		-	X	X	-	-	2
R0201	-		X	-	X	X	3
R0204	X	X		X	-	-	3
R0206	X	-	-		-	-	1
R0301	X	X	-	-		X	3
R0403	X	-	-	-	-		1
Total of effects	4	2	2	2	1	2	

Source: Self-made.

Analysis of relationships among the major risks in Table 9, showed that if cause risks linked to the loss of personal moral integrity (R0201), labor fluctuations (R0204), and the diffusion of unreliable information (R0301) are not managed, the effect risks will be stronger, with ensued lack of fulfillment of work objectives (R0101).

In step 5, considering the relevant risks, and the cause-effect relations, five control objectives were laid, which are linked to work objective No. 13: *To make advances in*

improvements of university management, based on a process approach, oriented to bettering quality and rationality, and integrated into the internal control system, in Key Result Area No. six: University management:

1. To conduct efficient human resources management that ensures staff suitability and motivation to perform their duties.
2. To strengthen the internal control system implemented at the university, based on proper analyses done to the control actions in the areas, depending on reliable statistics, and deadline completion under the required quality.
3. To implement quality process and procedures, in keeping with the policies and principles established to meet the management's goals.
4. To comply with the policies and procedures of information safety within quality parameters.
5. To comply with the rules established for Security and Protection.

In step 6, these control objectives were broken down into 12 actions. Seven actions for the objective linked to efficient management of human resources; two actions for strengthening the internal control system implemented at the university; and one action for all the others.

CONCLUSIONS

Risk management is a necessary work tool so that the top executives have reasonable confidence in that the utilization of resources is contributing to the efficiency and efficacy of the processes in the organization.

The procedure designed facilitates the implementation of risk management and prevention by UCI executives and staff with little training in risk management, according to CGR Resolution No. 60/11, and it contributes to strengthening the internal control system in all its respective areas. It can be applied to other higher education institutions.

The advantages of implementing this procedure are ensuring a systematic approach on management and prevention; diagnostic and further designing of a risk map of all the

facilities; the outcome is a prevention plan, which it facilitates continuous monitoring and reviewing.

The implementation of the procedure at the Internal Control Office, University of Computer Sciences, contributed to the identification of 15 risks and 48 associated causes, and during the analysis, 6 major risks and 5 control objectives; and 12 actions, were determined.

REFERENCES

Albanese, D. E. (2012). Análisis y evaluación de riesgos: aplicación de una matriz de riesgo en el marco de un plan de prevención contra el lavado de activos. *Revista Base (Administração e Contabilidade) da UNISINOS, 9*(3), 206-215. doi: 10.4013/base.2012.93.01

Alfonso, D. (2007). *Modelo de dirección estratégica para la integración del sistema de dirección de la empresa* (tesis doctoral en Ciencias Técnicas). Instituto Superior Politécnico *José Antonio Echeverría*, La Habana, Cuba.

Almuiñas, J. L., y Galarza, J. (2016a). Dirección estratégica y gestión de riesgos en las universidades. *Revista Cubana de Educación Superior, 35*(2), 83-92.

Almuiñas, J. L., y Galarza, J. (2016b). La gestión de riesgos: una alternativa para apoyar la gestión universitaria con enfoque estratégico. *Congreso Universidad, 5*(6), 92-110.

Bolaño, Y. (2014). *Modelo de dirección estratégica basado en la administración de riesgos para la integración del sistema de dirección de la empresa* (tesis doctoral en Ciencias Técnicas). Instituto Superior Politécnico *José Antonio Echeverría*, La Habana, Cuba.

Bolaño, Y., Alfonso, D., Pérez, A., y Arias, M. (2014). Modelo de dirección estratégica basado en la administración de riesgos. *Ingeniería Industrial, 35*(3), 344-357.

Comité Técnico ISO/TC 176. (2015). Norma Internacional ISO 9001-2015 Sistemas de gestión de la calidad - Requisitos.

Contraloría General de la República de Cuba. (3 de marzo de 2011). Resolución No. 60/11 "Normas del Sistema de Control Interno". La Habana, Cuba: Gaceta Oficial de la República de Cuba.

Mendoza, A. L., Bolaño, Y. y Mendoza, A. E. (2017). Procedimiento de gestión integrada de riesgos para el control interno universitario. *Revista ECA Sinergia, 8*(2), 80-98. DOI: https://doi.org/10.33936/eca_sinergia.v8i2.1012

Palma, C. (2011). ¿Cómo construir una matriz de riesgo operativo? *Revista de Ciencias Económicas, 29*(1), 629-635.

Rodríguez, H., Fernández, A. y de Dios Martínez, A. (2015). Sobre el análisis de la gestión presupuestaria con enfoque de riesgos. *Retos de la Dirección, 9*(1), 23-44.

Sulca, G. C., y Becerra, E. R. (2017). Control interno. Matriz de riesgo: Aplicación metodología COSO II. *Revista Publicando, 4*(12), 106-125.

Torres, C., Malta, N., Zapata, C. y Aburto, V. (2015). Metodología de gestión de riesgo para procesos en una institución de salud previsional. *Universidad, Ciencia y Tecnología, 19*(75), 98-109.

Varela, N., Oquendo, H., Romero, P. L. y Zúñiga, L. M. (2019). Toma de decisiones en la gestión integral del riesgo por sequía en Cuba. Retos de la Dirección, 13(1), 48-68.

Conflicts of interest and conflict of ethics statement

The authors declare that this manuscript is original, and it has not been submitted to another journal. The authors are responsible for the contents of this article, adding that it contains no plagiarism, conflicts of interest or conflicts of ethics.

Author contribution statement

Juan Fuentes Bauta: Theoretical background, design and development of the procedure, design of the manuscript and redaction of the manuscript, analysis of results, redaction of the conclusions and abstract.

Yuniel Bolaño Rodríguez: Content analysis and review of the manuscript. Analysis of results