

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

### Procedure for Integrated Risk Management at the University of Computer Sciences

Juan Fuentes Bauta<sup>1\*</sup> <http://orcid.org/0000-0003-0095-2047>

Dr. C. Yuniel Bolaño Rodríguez<sup>2</sup> <http://orcid.org/0000-0001-9391-2516>

<sup>1</sup> Universidad de las Ciencias Informáticas, La Habana, Cuba [jbauta@uci.cu](mailto:jbauta@uci.cu)

<sup>2</sup> Universidad Tecnológica de La Habana José Antonio Echeverría, La Habana, Cuba.

[ybolanor@ind.cujae.edu.cu](mailto:ybolanor@ind.cujae.edu.cu)

\*Autor para la correspondencia: [jbauta@uci.cu](mailto:jbauta@uci.cu)

#### 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.

## **ABSTRACT**

**Objective:** 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 forms of risk identification, analysis, and quantification that might take place in every process and event, and have a negative impact on the fulfillment of objectives. Another important result is the protection of resources, and the observance of laws and regulations, so that the strategic and work objectives are met. 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.

Recibido: 25/04/2019

Aprobado: 13/05/2020

## INTRODUCCIÓN

En la actualidad las universidades deben hacer frente a numerosos riesgos, dada la multitud de actividades que se desarrollan diariamente en un entorno (internacional, nacional, regional y local) dinámico e incierto, por lo que se hace necesario mejorar modelos de gestión (Almuiñas y Galarza, 2016a).

En función de lograr mejoras en su desempeño organizacional, se hace necesaria la implementación de un sistema de control interno inherente a todos los procesos, actividades y operaciones que se realizan en las instituciones de educación superior. Este sistema debe basarse en un enfoque preventivo que permita identificar con antelación los eventos o efectos adversos que de ocurrir impactan de forma negativa en el cumplimiento de los objetivos, la utilización y rendimiento de los recursos, así como en el cumplimiento del marco legal y regulatorio. Para lograr ese enfoque preventivo y contribuir a la mejora de los niveles de eficacia y eficiencia, es necesario desarrollar un

proceso de gestión de riesgos que permita identificar, analizar, evaluar y tratar los principales riesgos que afectan el desempeño y funcionamiento del sistema de control interno (Mendoza, Bolaño y Mendoza, 2017).

En este sentido, la Dirección de Control Interno (DCI) subordinada a la Vicerrectoría Primera, es la encargada de atender metodológicamente la gestión del control interno en la Universidad de la Ciencias Informáticas (UCI), el cual se materializa en cada una de las unidades organizativas de la institución, teniendo como misión evaluar, asesorar y supervisar la implementación del sistema de control interno con profesionales de principios y valores éticos, que garantice la seguridad razonable en el logro de los procesos de la Universidad, asegurando un eficiente uso y control de los recursos asignados bajo el cumplimiento de las regulaciones y leyes vigentes.

En acciones de control realizadas por la DCI se detectaron problemas en la determinación de los objetivos de control a partir de los principales riesgos, así como en la conformación del plan de prevención y una inadecuada administración de riesgos, ya sea por la poca preparación de los especialistas que deben aplicar las actividades de gestión de riesgos o por la pobre cultura al respecto que limita los análisis a cualquier nivel de la entidad, elementos que son considerados requisitos necesarios para alcanzar sus objetivos, la protección de sus recursos y el cumplimiento del marco legal y regulatorio.

En función de estos aspectos se propone como objetivo: elaborar un procedimiento para la gestión integrada de riesgos en la UCI, como parte del fortalecimiento del sistema de control interno (SCI), teniendo en cuenta los cambios de escenarios ocurridos e investigaciones realizadas a la gestión de riesgos, de tal manera que facilite a cuadros y

especialistas la implementación del componente gestión y prevención de riesgos de la Resolución 60/11 de la Contraloría General de la República (CGR) y le proporcione una herramienta para la gestión de riesgos en los procesos y actividades que pueden afectar el cumplimiento de los objetivos y metas trazados en cada una de las áreas. Para ello se realizó una revisión bibliográfica y documental, así como el análisis de resultados de investigaciones y entrevistas.

## **DESARROLLO**

### **Bases teóricas de la gestión integrada de riesgos**

Las organizaciones avanzan hacia un marco integrado de control con un enfoque integral, que implica a toda la plantilla, basado en el uso de una serie de herramientas para lograr un control interno efectivo, enmarcado en una filosofía de trabajo enfocada en la mejora continua mediante definiciones de estrategias (Alfonso, 2007; Bolaño, 2014; Contraloría General de la República de Cuba [CGR], 2011). Dentro de este marco está la gestión integral del riesgo la cual consiste, básicamente, en detectar oportunamente los diversos riesgos que pueden afectar a la organización para, de esta forma, generar estrategias que se anticipen a ellos, con el objetivo de convertirlos en oportunidades que contribuyan a la eficacia y eficiencia en sus operaciones, cumpliendo con las leyes y normativas establecidas y le permita alcanzar la misión y visión.

Esta gestión integral de riesgos implica analizar el contexto interno y externo de la organización y también requiere de un adecuado control interno. En Cuba se establece la Resolución No. 60/2011 de la CGR para las Normas del Sistema de Control Interno, con el fin de alcanzar resultados de eficiencia, orden y disciplina; por lo tanto, se hace

necesario crear una cultura de control y lograr que se tome conciencia acerca de su importancia.

CGR (2011) define el control interno como un proceso integrado a las operaciones, con un enfoque de mejoramiento continuo, extendido a todas las actividades inherentes a la gestión, efectuado por la dirección y el resto del personal; añade que se implementa mediante un sistema integrado de normas y procedimientos, que contribuyen a prever y limitar los riesgos internos y externos, proporciona una seguridad razonable al logro de los objetivos institucionales y una adecuada rendición de cuentas.

Otro componente describe la gestión y prevención de riesgos para el SCI, donde declara que el Plan de Prevención de Riesgos (PPR) constituye un instrumento de trabajo de la dirección para dar seguimiento sistemático a los objetivos de control determinados, se actualiza y analiza periódicamente con la activa participación de los trabajadores y ante la presencia de hechos que así lo requieran (CGR, 2011).

Por lo tanto, el sistema de control interno debe ser un espacio de la alta dirección para integrar todos los riesgos de una organización. De esta manera puede entenderse la gestión de riesgos como un proceso iterativo que parte de las políticas de la organización y que, utilizando los recursos y las tecnologías existentes, desarrolla un conjunto de actividades como: la identificación, análisis y evaluación de riesgos, toma de decisiones basadas en el costo/beneficio donde a través de acciones se busca: impedir, eliminar, reducir y controlar los efectos adversos (riesgos) que se materializan en los procesos de la organización y que afectan su desempeño (Bolaño, 2014)

Estudios teóricos y prácticos realizados en la gestión de riesgos (Bolaño, 2014; Bolaño, Alfonso, Pérez y Arias, 2014; Mendoza *et al.*, 2017; Rodríguez, Fernández y de Dios,

2015; Varela, Oquendo, Romero y Zúñiga, 2019) enfatizan en que la aplicación del enfoque integral de riesgos posibilitará la anticipación en la toma de decisiones con enfoques sistémico, estratégico y participativo.

### **Procedimiento para la gestión de riesgos en la Universidad de las Ciencias Informáticas**

Cada área, con la participación de todos los trabajadores, realizará la identificación, análisis y evaluación de los riesgos que puedan afectar el cumplimiento de sus objetivos y metas, vinculándolos con las causas y condiciones que lo generan y los objetivos de control; luego determinarán los riesgos que van a formar parte de su plan de prevención.

A continuación se presentan las diferentes bases teóricas relacionadas con el procedimiento para la gestión integrada de riesgos, como parte del fortalecimiento del sistema de control interno. Esta se nutre de diferentes elementos teóricos desarrollados por Bolaño (2014) en su tesis de doctorado, así como de las normas del SCI expuestas en la Resolución 60/2011 de la CGR.

Conceptos claves:

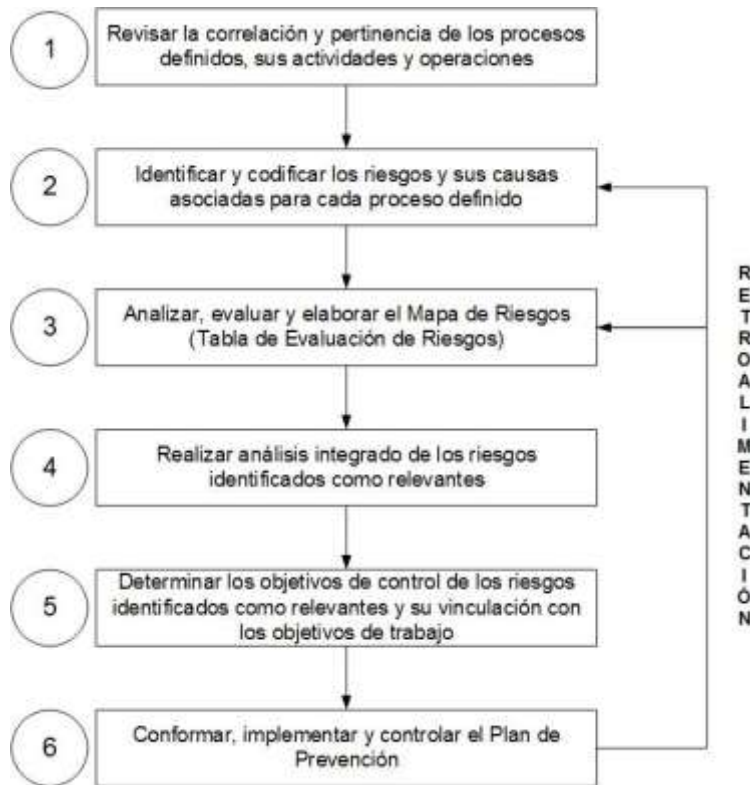
Proceso: Conjunto de actividades relacionadas entre sí o que interactúan, transformando elementos de entrada en elementos de salida (producto/servicio). (Comité Técnico ISO/TC 176, 2015).

Riesgo: Probabilidad de que ocurra un efecto no deseado en los procesos de la organización, que traen consigo un impacto negativo. (Bolaño, 2014)

Causas de riesgo: Son elementos que hacen posible la ocurrencia del riesgo. Las causas de riesgos pueden ser: situaciones, fenómenos, omisiones, violaciones de lo establecido, decisiones, factores externos e internos, eventos, cambios inesperados (Bolaño, 2014).

Objetivos de control: son el resultado o propósito que se desea alcanzar con la aplicación de procedimientos de control, los que deben verificar los riesgos identificados y estar en función de la política y estrategia de la organización (CGR, 2011).

El procedimiento para la gestión integrada de riesgos en la UCI como parte del fortalecimiento del sistema de control interno se desarrolla a través de seis pasos, como se observa en la Fig.1.



Fuente: Elaboración propia.

**Fig. 1.** Procedimiento para la gestión integrada de riesgos

*Paso 1:* Revisar la correlación y pertinencia de los procesos definidos, sus actividades y operaciones.

Toda actividad que la entidad desarrolla debe estar incluida en alguno de sus procesos, por lo que se reconoce el enfoque de proceso como la forma de entender el



funcionamiento de la organización y que este incluye actividades y operaciones. Los procesos ocurren en la organización, independientemente de si se gestionan o no. Cuando no se gestionan, lo más frecuente es que se afecte la eficacia y eficiencia de estos y por ende de los objetivos estratégicos. Mejor sería identificar los procesos, analizarlos, gestionarlos y mejorarlos (Alfonso, 2007).

En este paso se deben revisar los procesos definidos en la entidad o área, determinar las actividades de cada uno de los identificados y verificar las actividades u operaciones que incidan en el cumplimiento de los objetivos de la entidad o áreas.

*Paso 2:* Identificar y codificar los riesgos y sus causas asociadas para cada proceso definido.

Se procede a la identificación de los riesgos y sus causas en cada uno de los procesos. Para identificar los riesgos en estos puede utilizarse la siguiente pregunta: ¿qué puede ocurrir en los procesos P1, P2, ..., Pn anteriormente definidos que pueda afectar el desempeño de la entidad o área?

Debe valorarse al identificarse el riesgo, que este impacte de forma negativa en el cumplimiento de los objetivos, en la protección de cualquier tipo de recurso, en el medio ambiente, en el cumplimiento de leyes y normativas a las cuales está sujeta la entidad, en el comportamiento ético de los trabajadores y dirigentes de la organización. A los riesgos identificados se les debe asignar una codificación, por ejemplo: el riesgo R0301, es el riesgo uno del proceso tres. Para la identificación de riesgos la organización puede tener en cuenta un grupo de elementos y criterios, según corresponda, que se exponen a continuación:

- ✓ Las causas y condiciones de las ilegalidades, hechos delictivos o de corrupción detectados, así como de las deficiencias detectadas por acciones de control internas o externas.
- ✓ Quejas y denuncias recibidas.
- ✓ Debilidades, amenazas, fortalezas y oportunidades (DAFO).
- ✓ Análisis de los incumplimientos en los balances de trabajo.
- ✓ Procesos: ficha de procesos, relaciones entre ellos y las variables de salida.
- ✓ Lista de riesgos identificados anteriormente en la entidad o área y los definidos en el modelo Perfiles de competencia de los puestos de trabajo.
- ✓ Los recursos de la entidad o área (humanos, materiales, tecnológicos, financieros, informativos).
- ✓ Leyes, normas o resoluciones que se tienen que cumplir.

Deben tenerse en cuenta en la identificación de los riesgos: los planes y/o reglamentos de seguridad informática, seguridad y salud del trabajo, y de seguridad y protección.

Deben tomarse en consideración, además, para identificar los riesgos:

- ✓ Dentro de un mismo proceso, un riesgo no puede ser causa de otro riesgo de forma directa.
- ✓ Un riesgo de un proceso puede ser una causa de un riesgo de otro proceso.
- ✓ Puede identificarse un riesgo en un proceso en el que dicho proceso no sea responsable por la ocurrencia del riesgo.

Se distinguen las causas externas e internas para cada uno de los riesgos identificados anteriormente. Es importante para reconocer las causas, reunir los criterios de todos los trabajadores involucrados en las actividades y operaciones de los procesos; debe

utilizarse las asambleas de rendición de cuenta y otros espacios de intercambio con los empleados. Las causas deberán codificarse también, por ejemplo: la causa C030102, es la causa dos, del riesgo uno identificado en el proceso tres.

*Paso 3:* Analizar, evaluar y elaborar el mapa de riesgos (tabla de evaluación de riesgos) (Tabla 5).

Después de identificados los riesgos, se miden a partir de la posibilidad de ocurrencia e impacto estimados. El análisis de riesgos es un proceso cognoscitivo en el cual, usando sistemáticamente la información disponible, se podrá determinar cuan probable o posible es que se presente un evento determinado y la magnitud de sus consecuencias o impactos, para proveer datos que son utilizados en la evaluación y tratamiento de estos (Albanese, 2012; Bolaño, 2014; Palma, 2011; Sulca y Becerra, 2017; Torres, Malta, Zapata y Aburto, 2015).

Estimar la probabilidad de ocurrencia del riesgo:

La estimación de la probabilidad se determina por la media geométrica entre los valores del nivel de incidencia ( $ni$ ) de las causas del riesgo sobre la ocurrencia de este y el nivel de descontrol ( $nd$ ) sobre las causas del riesgo. Se puede expresar por la ecuación siguiente:

$$P = \sqrt[2]{ni * nd} \quad \text{donde} \quad 0 \leq ni \leq 1 \quad 0 \leq nd \leq 1$$

Los valores de  $ni$  y  $nd$ , se pueden obtener de las descripciones que aparecen en las Tablas 1 y Tabla 2.

**Tabla 1.** Determinación del nivel de incidencia de las causas del riesgo sobre la ocurrencia de este

Descripción del nivel de incidencia de las causas o factores de riesgos sobre su ocurrencia	Evaluación
Las causas o factores de riesgos inciden totalmente y con la máxima potencia sobre la ocurrencia del riesgo.	1,0

Las causas o factores de riesgos inciden casi totalmente con alta potencia sobre la ocurrencia del riesgo.	0,9
Las causas o factores de riesgos inciden bastante con alta potencia sobre la ocurrencia del riesgo.	0,8
Las causas o factores de riesgos inciden bastante con potencia casi alta sobre la ocurrencia del riesgo.	0,7
Las causas o factores de riesgos inciden medianamente con potencia ligeramente superior a la moderada sobre la ocurrencia del riesgo.	0,6
Las causas o factores de riesgos inciden medianamente y con potencia moderada sobre la ocurrencia del riesgo.	0,5
Las causas o factores de riesgos inciden casi medianamente y con potencia ligeramente inferior a la moderada sobre la ocurrencia del riesgo.	0,4
Las causas o factores de riesgos inciden casi medianamente con baja potencia sobre la ocurrencia del riesgo.	0,3
Las causas o factores de riesgos inciden poco y con baja potencia sobre la ocurrencia del riesgo.	0,2
Las causas o factores de riesgos casi no inciden y con muy baja potencia sobre la ocurrencia del riesgo.	0,1
Las causas o factores de riesgos no inciden (no hay riesgo).	0,0

Fuente: (Bolaño, 2014)

**Tabla 2.** Determinación del nivel de descontrol sobre las causas de los riesgos

Descripción del nivel de descontrol sobre las causas o factores de riesgos	Evaluación
Las causas o factores de riesgos no se controlan.	1,0
Las causas o factores de riesgos casi no se controlan.	0,9
Las causas o factores de riesgos se controlan poco, con muy baja efectividad sobre la ocurrencia del riesgo.	0,8
Las causas o factores de riesgos se controlan poco, con baja efectividad sobre la ocurrencia del riesgo.	0,7
Las causas o factores de riesgos se controlan medianamente, con baja efectividad sobre la ocurrencia del riesgo.	0,6
Las causas o factores de riesgos se controlan medianamente, con niveles intermedios de efectividad sobre la ocurrencia del riesgo.	0,5
Las causas o factores de riesgos se controlan medianamente, con efectividad ligeramente superior a los niveles intermedios.	0,4
Las causas o factores de riesgos se controlan bastante, con efectividad casi alta sobre la ocurrencia del riesgo.	0,3
Las causas o factores de riesgos se controlan bastante, con alta efectividad sobre la ocurrencia del riesgo.	0,2
Las causas o factores de riesgos se controlan casi totalmente con muy alta efectividad.	0,1
Las causas del riesgo se controlan totalmente con excelente efectividad por lo que el riesgo no ocurre (no hay riesgo).	0,0

Fuente: (Bolaño, 2014)

Para la estimación del impacto se tendrá en cuenta la tabla tres.

**Tabla 3.** Estimación del impacto

Categoría	Descripción	Evaluación
Catastrófico	Daños severamente serios en el desempeño del proceso	10 9
Muy alto	Daños muy importantes al desempeño del proceso	8 7
Alto	Daños importantes al desempeño del proceso	6 5
Medio	Impactará moderadamente en el proceso	4 3

Bajo	Impacto mínimo en el desempeño del proceso	2 1
No impacta	No impacta en el desempeño del proceso	0

Fuente: Elaboración propia

Para evaluar el nivel de prioridad del riesgo (NPR) se procede a calcular el valor del riesgo (VaR); se usan las variables probabilidad de ocurrencia del riesgo ( $0 < P < 1$ ) a y el impacto estimado (I), mediante la siguiente expresión:

$$VaR = P * I$$

Donde:

VaR = Valor del riesgo (en puntos).

P = Probabilidad estimada del riesgo ( $0 < P < 1$ ).

I = Impacto estimado del riesgo (en puntos).

Una vez calculado el valor del riesgo se procede a ubicarlo en el rango de valor del riesgo como se muestra en la Tabla 4 y se determina el NPR.

**Tabla 4.** Nivel de prioridad del riesgo

Rango de valor del riesgo	Nivel de prioridad del riesgo (NPR)	Observaciones
$VaR \geq 6,4$	Extremo	Deben aparecer en el plan de prevención.
$3,6 \leq VaR < 6,4$	Alto	
$1,5 \leq VaR < 3,6$	Moderado	Evaluar en el área si se lleva o no al plan de prevención.
$0,6 \leq VaR < 1,5$	Bajo	Implementar acciones a largo plazo que reduzcan o eliminen el riesgo. Se tiene en el mapa de riesgos pero no va al plan de prevención.
$VaR < 0,6$	Trivial	Se tiene en el mapa de riesgo pero no va al plan de prevención

Fuente: Elaboración propia.

Luego se procede a elaborar el mapa de riesgos (tabla de evaluación de riesgos) con los datos obtenidos según muestra la tabla cinco.

**Tabla 5.** Mapa de riesgos (tabla de evaluación de riesgos)

Proceso	Riesgos	Causas	Análisis	NPR
---------	---------	--------	----------	-----

	Código	Descripción	Código	Descripción	P	I	VaR	
--	--------	-------------	--------	-------------	---	---	-----	--

Fuente: Elaboración propia

En los casos que sean posibles, cuantificar una valoración estimada de la afectación o pérdida de cualquier índole que pudiera ocasionarse.

*Paso 4:* Realizar análisis integrado de los riesgos identificados como relevantes.

En este paso se determinan los principales riesgos de la entidad o área y se realiza un análisis integrado de estos, sobre la base de las relaciones de causa y efecto que se pueden establecer. Para esto es necesario analizar las causas comunes y si un riesgo de un proceso es una causa para otro identificado en otro proceso o viceversa. También se debe analizar las relaciones lógicas que se establecen entre los riesgos, a partir de las relaciones entre las actividades que generan los riesgos.

Para representar las relaciones de causa y efecto entre los principales riesgos de la entidad o área, se puede utilizar la matriz de relaciones de riesgos (ver ejemplo en la Tabla 6). Con este ejemplo se puede redactar como situación crítica a través de una hipótesis, que si no se logra una reducción efectiva de los riesgos causas, entonces se agudizará aún más la ocurrencia y el impacto asociados a los riesgos efectos.

**Tabla 6:** Ejemplo de matriz de relaciones entre los principales riesgos

	Riesgo 1	Riesgo 2	Riesgo n	Total de causas
Riesgo 1				
Riesgo 2				
Riesgo n				
Total de efectos				

Fuente: Modificación a partir de (Bolaño, 2014)

Los riesgos que hayan sido evaluados de extremos, altos o moderados (hasta un 50 % del total de riesgos), son los candidatos a ser seleccionados como principales y constituyen elementos a considerarse en los objetivos de control de la entidad o área.

*Paso 5:* Determinar los objetivos de control de los riesgos identificados como relevantes y su vinculación con los objetivos de trabajo.

Cada área debe diseñar los objetivos de control para minimizar los riesgos identificados como relevantes y vincularlos con los objetivos de trabajo para el logro de la eficiencia, eficacia, control de los recursos y cumplimiento de las legislaciones. El objetivo de control se genera y enuncia tomando la versión negativa de la amenaza y convirtiéndola en una declaración positiva de deseo, es decir, analizando qué puede ocurrir incorrectamente y qué se propone para que no ocurra.

*Paso 6:* Conformar, implementar y controlar el plan de prevención.

A partir de los objetivos de control se elabora entonces en el paso seis y último, el plan de prevención (Tabla 7), cuyas acciones van dirigidas al cumplimiento de los objetivos de control que a su vez pone su punto focal en la reducción de los riesgos relevantes y sus relaciones. También este paso abarca la implementación de dicho plan donde es esencial el liderazgo y la motivación de los dirigentes y trabajadores. En la propia ejecución de las acciones del plan de prevención pueden originarse otros riesgos no considerados o puede que cambien las variables de probabilidad e impacto, de ahí que el procedimiento tenga una retroalimentación a los pasos dos y tres.

**Tabla 7:** Propuesta de plan de prevención

Proceso	Objetivos de control	Riesgos		Causas		Acciones	Responsable	Ejecutante	Fecha de cumplimiento
		Código	Descripción	Código	Descripción				

Fuente: Elaboración propia

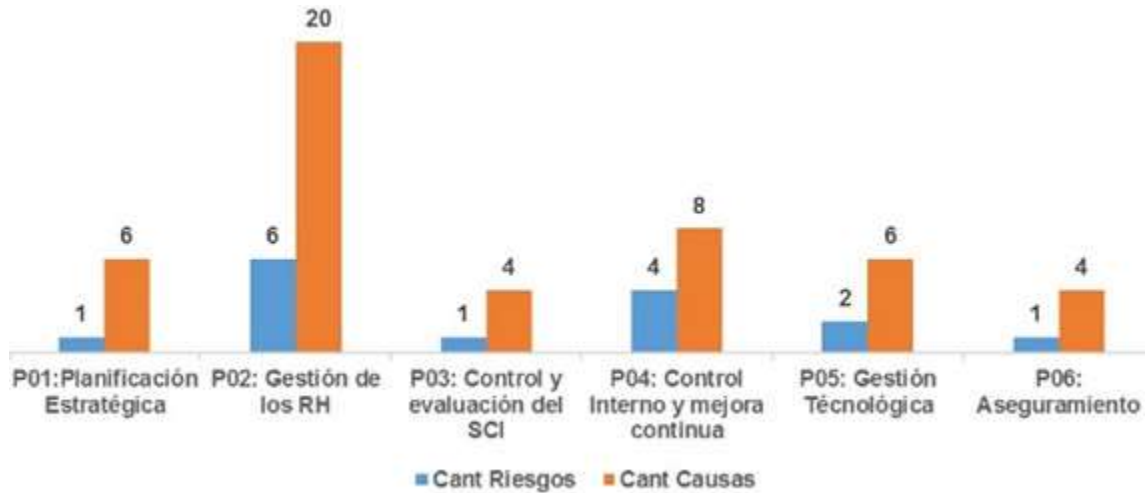
El plan de prevención consolidado a nivel de vicerrectorías, direcciones generales, facultades y direcciones con áreas subordinadas no es la suma de los riesgos definidos en los planes de prevención de sus áreas subordinadas, sino el resultado del análisis de los que pongan en peligro el cumplimiento de sus objetivos y misión; así mismo se conformará el consolidado a nivel de universidad, el cual debe ser revisado y aprobado en la instancia correspondiente.

### Resultados

El procedimiento fue aplicado en la DCI de la Universidad de las Ciencias Informáticas. Arrojó los siguientes resultados por cada paso del procedimiento.

En el paso uno se identificaron siete procesos (dos claves y cinco funcionales) y al aplicar el paso dos se identificaron 15 riesgos y 48 causas asociados a estos, siendo el proceso de gestión de los recursos humanos donde más riesgos se identificaron (seis y 20 causas), seguido por el proceso control interno y mejora continua con cuatro riesgos y ocho causas (Fig. 2).





Fuente: Elaboración propia

**Fig.2:** Identificación de riesgos por procesos

En el paso tres se analizó cada uno de los riesgos identificados anteriormente; se evaluó la probabilidad e impacto estimado, el valor del riesgo y el nivel de prioridad de cada uno. Se obtuvieron: dos riesgos altos, cuatro moderados, siete bajos y dos riesgos triviales. Con los principales riesgos (Tabla 8) —representan el 40 % de los riesgos identificados— se ejecuta el paso cuatro realizando un análisis integrado, donde la atención se centra más en el conjunto de riesgos, que en cada uno por separado. Las relaciones de causa y efecto entre estos riesgos se determinan con la matriz de relaciones. Esto se puede observar en la Tabla 9.

**Tabla 8.** Principales riesgos

Proceso	Riesgos	
	Código	Descripción
P01: Planificación estratégica	R0101	Incumplimiento de los objetivos de trabajo
P02: Gestión de los recursos humanos	R0201	Pérdida de la integralidad moral
	R0204	Fluctuación laboral
	R0206	Afectación de la salud de los trabajadores
P03: Control y evaluación del sistema de control implementado en la universidad	R0301	Emisión de información no confiable.
P04: Control interno y mejora continua	R0403	Pérdida de documentos relevantes

Fuente: Elaboración propia.

**Tabla 9.** Matriz de relaciones entre los principales riesgos

	R0101	R0201	R0204	R0206	R0301	R0403	Total de causas
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 de efectos	4	2	2	2	1	2	

Fuente: Elaboración propia.

Al analizar las relaciones entre los principales riesgos en la Tabla 9, se puede destacar que, si no se gestionan los riesgos causas relacionados con la pérdida de la integridad moral (R0201), la fluctuación laboral (R0204) y la emisión de información no confiable (R0301); entonces se agudizarán aún más los riesgos efectos: el incumplimiento de los objetivos de trabajo (R0101).

En el paso cinco —teniendo en cuenta los riesgos relevantes y las relaciones de causas y efectos entre ellos— se formularon cinco objetivos de control que se exponen a continuación; estos se vinculan con el objetivo de trabajo 13 “Lograr avances en el perfeccionamiento de la gestión universitaria con un enfoque de procesos, orientado a la calidad y racionalidad e integrado al sistema de control interno” del Área de Resultado Clave seis “Gestión Universitaria”:

1. Efectuar una gestión eficiente de los recursos humanos que garantice la idoneidad y motivación de trabajadores en sus respectivas responsabilidades.
2. Fortalecer el sistema de control interno implementado en la universidad a partir de análisis correctos realizados según estadísticas confiables y del cumplimiento en tiempo y con la calidad requerida, de las acciones de control a las áreas.

3. Ejecutar con calidad los procesos y procedimientos cumpliendo con las políticas y principios establecidos para el logro de los objetivos de la Dirección.
4. Cumplir con calidad las políticas y procedimientos de seguridad informática.
5. Cumplir con las indicaciones de la Seguridad y Protección establecidas.

Para el paso seis, estos objetivos de control se desagregaron en 12 acciones; para el objetivo relacionado con la gestión eficiente de los recursos humanos, siete acciones; para el fortalecimiento del sistema de control interno implementado en la universidad, dos acciones y para los restantes una acción.

## **CONCLUSIONES**

La gestión de riesgos constituye una herramienta de trabajo indispensable para que la alta dirección pueda tener una razonable confianza en que la utilización de los recursos está tributando a la eficiencia y eficacia en el cumplimiento de los procesos de la organización.

El procedimiento diseñado facilita la implementación del componente gestión y prevención de riesgos a directivos y trabajadores de la UCI con poca preparación en la gestión de riesgos, teniendo en cuenta lo establecido en la Resolución 60/11 de la CGR y tributa a su vez, al fortalecimiento del sistema de control interno en sus respectivas áreas. Puede aplicarse en otras instituciones de educación superior.

La ejecución del procedimiento tiene como ventajas: asegurar un enfoque sistemático de gestión y prevención; el diagnóstico y posterior elaboración del mapa de riesgos de cada

una de las áreas; se obtiene como modelo final el plan de prevención y facilita el continuo monitoreo y revisión.

La aplicación del procedimiento en la Dirección de Control Interno de la Universidad de las Ciencias Informáticas logró identificar 15 riesgos y 48 causas asociados a estos; y en el análisis se determinaron seis riesgos relevantes, cinco objetivos de control y 12 acciones.

## REFERENCIAS

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](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.

### **Declaración de conflicto de interés y conflictos éticos**

Los autores declaramos que el presente manuscrito es original y no ha sido enviado a otra revista. Los autores somos responsables del contenido recogido en el artículo, y en él no existen: ni plagios, ni conflictos de interés, ni éticos.

### **Declaración de contribuciones de los autores**

Juan Fuentes Bauta: Fundamentos teóricos, diseño y desarrollo del procedimiento, diseño del artículo, redacción y análisis de los resultados, elaboración de las conclusiones y resumen.

Yuniel Bolaño Rodríguez: Análisis y revisión de todo el contenido. Análisis de resultados.