Clío América/ Vol. 12, No. 24 - 2018 / 198 - 211
DOI: http://dx:10.21676/23897848.2868

EVALUACIÓN DEL RIESGO INICIAL EN UN PROCESO MISIONAL DE UNA CAJA DE COMPENSACIÓN FAMILIAR CON BASE EN LA NORMA NTC-ISO 31000:2011

EVALUATION OF INITIAL RISKS IN THE MISSION PROCESS OF A BENEFIT SOCIETY CREDIT BASED ON THE NTC-ISO 31000: 2011 STANDARD

Jeniffer Tatiana Orozco-Sánchez[1], Adriana Castro-Rivera[2] y Gerardo Martínez-Díaz[3]

Tipología: Artículo de investigación científica y tecnológica
Para citar este artículo: Orozco, S. J., Castro, R. A. y Martínez, D. G. (2018). Evaluación del riesgo inicial en un proceso misional de una caja de compensación familiar con base en la norma NTC-ISO 31000:2011. *Clío América*, *12*(24), 198 - 211. doi: http://dx.doi.org/10.21676/23897848.2868

Recibido en agosto 24 de 2018
Aceptado en 26 de octubre de 2018
Publicado en línea en 28 de noviembre de 2018

RESUMEN

La administración del riesgo es un proceso sistemático y proactivo que proporciona a las organizaciones un conjunto de estrategias diseñadas para identificar aquellos eventos potenciales que pueden impactar negativamente el cumplimiento de los objetivos institucionales. Este artículo evalúa el nivel de criticidad del riesgo inicial en el proceso de gestión de aportes de la Caja de Compensación Familiar Cf desde la perspectiva NTC ISO 31000:2011. Mediante análisis documental, observación directa y lluvia de ideas como modalidad de entrevista, se identificaron 35 causas concretas de 9 riesgos potenciales, así como los posibles efectos que podría afrontar la corporación. Los resultados indican que es conveniente aplicar la metodología NTC ISO 31000 para estimar la magnitud de los riesgos a que está expuesta la Caja de Compensación Familiar Cf, lo cual puede demostrar que (i) permite aumentar la probabilidad de alcanzar los objetivos propuestos al administrar adecuadamente los riesgos y (ii) permite prevenir pérdidas económicas, de información o reputacionales asociadas a la materialización de eventos negativos sobre la organización, mejorando la eficacia y eficiencia operacional. Este estudio podría ser utilizado como una referencia para gestionar los riesgos en cualquier organización, independiente de su naturaleza o tamaño.

Palabras clave: NTC ISO 31000:2011 – riesgo – riesgo organizacional – caja de compensación.
JEL: M1, M5.

ABSTRACT

Risk management is a proactive, systematic process that provides organizations with a set of strategies designed to identify events that can have a negative impact on the achievement of the institution's goals. This article evaluates initial critical risk levels in the process of managing the contributions of the Benefit Society Credit Union Cf from the perspective of NTC ISO 31000:2011. Documental analysis, direct observation, and brainstorming as interviewing methods made it possible to identify 35 concrete causes of 9 potential risks, as well as the potential consequences a corporation can face. The results indicate that it is advisable to apply the NTC ISO 31000 methodology to estimate the extent of the risk the Benefit Society Credit Union Cf is exposed to. Said methodology can demonstrate that (i) it increases the chances of achieving set goals by properly managing risks; and it (ii) prevents financial, information, or reputation losses associated with the materialization of negative events for the organization. This has improved the efficacy and efficiency of the operation. This study can be used as a reference to manage risks in any organization, regardless of their size or nature.

Keywords: NTC ISO 31000:2011 standard – risk – organizational risk – Compensation Fund.

1 Universidad de la Amazonia. Colombia. Correo: tatisorozks@hotmail.com. ORCID: http://orcid.org/0000-0003-4602-481X
2 Universidad de la Amazonia. Colombia. Correo: adricasri@hotmail.com. ORCID: http://orcid.org/0000-0002-7497-9296
3 Universidad Santo Tomás. Colombia. Correo: gerardo.martinezdiaz@gmail.com. ORCID: http://orcid.org/0000-0002-7837-8156

INTRODUCCIÓN

En Colombia, el ambiente organizacional en que las cajas de compensación familiar desarrollan sus actividades está condicionado por la dinámica cambiante de los avances tecnológicos y la globalización. En este escenario volátil aparece la incertidumbre, caracterizada por la deficiencia de conocimiento sobre eventos adversos que pueden afectar el cumplimiento de la misión y los objetivos corporativos (Preve, 2015). Ante la necesidad de controlar estos eventos de una manera eficaz, surge entonces la administración de riesgos como "una disciplina necesaria para preservar las organizaciones y protegerlas de pérdidas que afecten su estabilidad" (Mejía y Villanueva, 2014, p. 123).
En los últimos años, la práctica de la administración del riesgo ha presentado una notable evolución, principalmente con los marcos de referencia propuestos por organismos internacionales, que se constituyen en herramientas integrales para ayudar a diversas entidades a enfrentar sus riesgos emergentes. Actualmente, existen diversos marcos internacionales que establecen los principios y lineamientos para que las organizaciones implementen un proceso de gestión de riesgos. Entre los principales podemos destacar la norma ISO 31000:2009 - Gestión de riesgos, principios y directrices, propuesta por la Organización Internacional de Normalización (ISO).

La norma ISO 31000:2009 precisa un "conjunto de actividades coordinadas para dirigir y controlar una organización con respecto al riesgo" (ISO, 2009, p. 9). Es tal su importancia que en 2011 fue adoptada para Colombia por el Instituto Colombiano de Normas Técnicas y Certificación mediante la NTC ISO 31000, que reemplazó la NTC 5254 de 2004 (Icontec, 2011).

En la revisión de la bibliografía pertinente a la investigación, se consideraron aquellos trabajos propuestos bajo la norma ISO 31000:2009 dado que esta sirvió de referente para la adopción de la NTC ISO 31000:2011 en Colombia. Estudios realizados por Espino (2014), Arías, Díaz y Vargas (2014), Castillo (2016) y Rodríguez (2016) coinciden en afirmar que esta norma es una herramienta efectiva para la gestión del riesgo en cualquier organización, independientemente de su naturaleza, facilitando una estructura que comprende desde la identificación, el análisis y la valoración de los riesgos hasta la formulación y el diseño de planes de acción para su seguimiento.

Se revisaron aplicaciones de la norma en trabajos de Valencia (2013), Uribe (2012), Oliver (2015), Zapata (2015), Lavielle (2016), Cervantes, Hernández y Reyes (2017) y García y Suárez (2017). Se destaca en particular el trabajo de Hinestroza y González (2018) en una caja de compensación familiar que cumple funciones complementarias del sistema de seguridad social colombiano, considerado como antecedente importante de esta investigación.

El problema de investigación se sustenta en la necesidad de verificar cómo la aplicación de la metodología NTC ISO 31000, en su versión 2011, permite evaluar el nivel de criticidad de los principales riesgos subyacentes a las actividades de gestión de aportes de la caja de compensación familiar Cf, lo cual puede contribuir a prevenir daños de equipos o de información, pérdidas económicas, posibles hechos de corrupción, retrasos en el desarrollo de los procesos misionales, demandas judiciales y sanciones económicas y disciplinarias. Esta investigación es pertinente porque busca verificar la aplicabilidad de la NTC ISO 31000:2011 en la determinación y evaluación de riesgos de un proceso misional de una entidad en particular (caja de compensación) que cumple funciones complementarias del sistema de seguridad social colombiano.

METODOLOGÍA

Esta investigación se desarrolló bajo un enfoque mixto que combina los tipos de investigación descriptivo, documental y de estudio de caso. En la revisión de fuentes de información se privilegió la consulta de artículos de investigación en bases de datos indexadas, trabajos de grado en repositorios

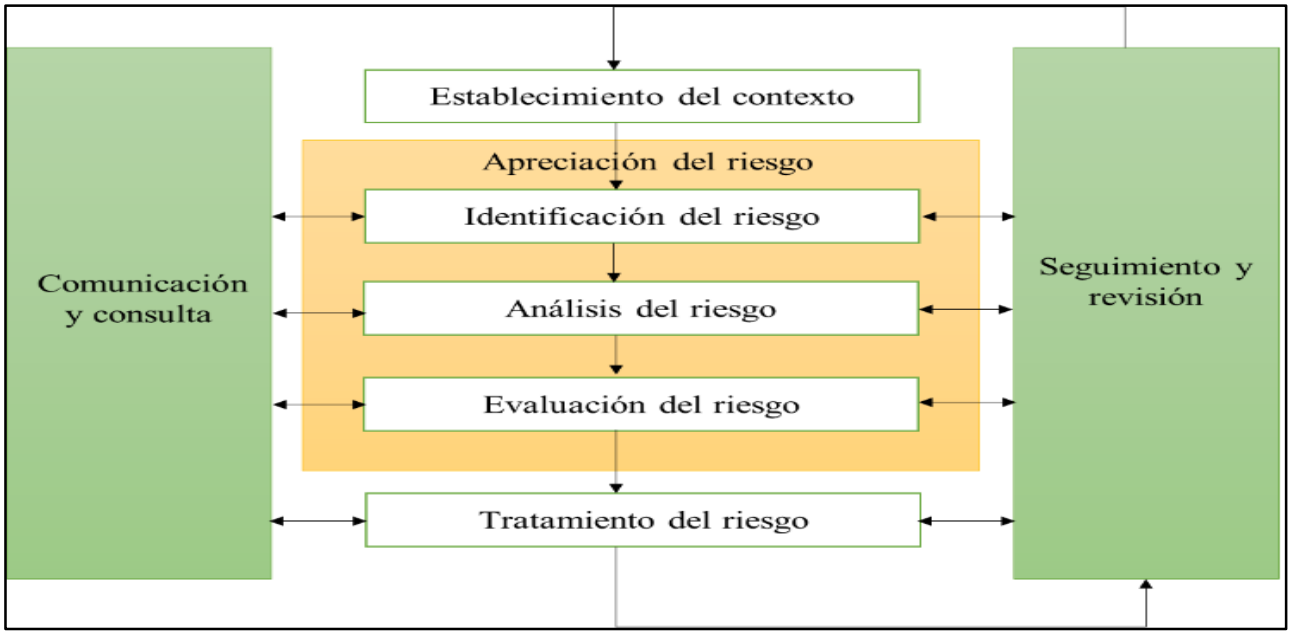
Clío América / ISSN 1909-941X / Vol. 12, No. 24, julio – diciembre de 2018
DOI: http://dx.doi.org/10.21676/23897848.2868

institucionales de universidades públicas y privadas en Colombia, normas internacionales y nacionales, además de documentos con literatura especializada sobre el tema de evaluación riesgos, lo que permitió ampliar y complementar el estado del arte sobre el tema objeto de esta investigación.

Metodología para la administración del riesgo NTC ISO 31000:2011

En la figura 1 se presenta la metodología para la administración integral del riesgo propuesta en la NTC ISO 31000:2011. Esta propone un conjunto de tareas interrelacionadas que incluye el establecimiento del contexto, la identificación, el análisis, la evaluación y el tratamiento del riesgo, y las actividades de comunicación y consulta y de seguimiento y revisión.

Figura 1. Proceso general de la gestión del riesgo



Fuente: elaboración propia basada en Icontec (2011).

A continuación se describen cada una de las actividades que conforman el proceso para la gestión del riesgo.

Comunicación y consulta (5.2). Esta actividad, transversal al proceso de gestión del riesgo, permite integrar a todas las partes involucradas y a las personas responsables de la administración de los riesgos en la organización con el fin de comprender la base de la gestión y sus planes y acciones con relación al riesgo.

La pertinencia de esta actividad radica en que permite conocer la percepción que tienen las partes interesadas sobre cada uno de los riesgos identificados. Nótese que estas opiniones pueden variar debido al contexto en el que se desarrollan las actividades de la organización; pueden existir así diferencias en los valores, las necesidades, los conceptos y los intereses de las partes.

Establecimiento del contexto (5.3). Esta actividad tiene como propósito efectuar un análisis de los factores internos y externos a la empresa que pueden influir en el cumplimiento de los objetivos de la institución (Mejía, 2004). Este proceso contempla dos aspectos: análisis del contexto externo y análisis del contexto interno.

El análisis del contexto externo incluye aspectos financieros, políticos, legales, reglamentarios, económicos, tecnológicos, sociales y culturales, entre otros, considerados fuentes potenciales de riesgo debido a que están por fuera del control de la organización (Lascano, Caro y Arcieri, 2008). Respecto al contexto interno, este abarca factores

Clío América / ISSN 1909-941X / Vol. 12, No. 24, julio – diciembre de 2018
DOI: http://dx.doi.org/10.21676/23897848.2868

como el compromiso de los empleados, la filosofía y cultura del riesgo, la autoridad, la responsabilidad, la integridad y los valores éticos, entre otros.

Identificación del riesgo. El propósito de esta actividad es identificar aquellos eventos que pueden afectar la capacidad de la organización para cumplir con los objetivos trazados. Es relevante determinar las fuentes de riesgo, las áreas de impacto, los eventos y sus causas y consecuencias potenciales (Icontec, 2011). En el desarrollo de este proceso se deben aplicar las herramientas y técnicas de identificación del riesgo que sean adecuadas a sus objetivos y capacidades, y a los riesgos que se enfrentan. Además, es importante involucrar al personal con el conocimiento idóneo ya que este dispone de la información pertinente y suficiente para "considerar qué podría suceder, cómo, cuándo y por qué" (Purdy, 2010, p. 884).

Análisis del riesgo. Esta actividad busca estimar la probabilidad de ocurrencia de cada riesgo identificado y medir la magnitud del impacto de presentarse, con el propósito de valorar el nivel de riesgo en función del grado de amenaza que representa para la organización (Pulido, 2015). En la tabla 1 se presentan los criterios de factibilidad adoptados por el Departamento Administrativo de la Función Pública (DAFP) para estimar la oportunidad de materialización de un riesgo. Estos criterios se asignan bajo una escala cualitativa representada por números de 0 a 5 como valor propio.

Tabla 1. Escala cualitativa de frecuencia de ocurrencia

Nivel	Descriptor	Descripción
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias.
3	Posible	El evento podrá ocurrir en algún momento.
2	Improbable	El evento puede ocurrir en algún momento.
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).

Fuente: elaboración propia basada en DAFP (2014).

En la tabla 2 se especifican los criterios propuestos por el DAFP para estimar el impacto esperado ante la materialización de una amenaza.

Tabla 2. Criterios de impacto definidos en la guía para la administración del riesgo DAFP v3

Niveles para calificar el impacto		Interrupción de operaciones	Pérdida de información	Entes de control
1	**Catastrófico**	>5 días	Total. Sin copia de seguridad	Intervención
2	**Mayor**	>2 días	Parcial o incompleta	Sanción
3	**Moderado**	1 día	Retraso en el restablecimiento de información por un día	Investigación penal, fiscal o disciplinaria
4	**Menor**	<1 día	Retraso en el restablecimiento de información por unas horas	Investigación disciplinaria
5	**Insignificante**	No se presenta	No existe pérdida de información	Sin sanciones

Fuente: elaboración propia basada en DAFP (2014).

Clío América / ISSN 1909-941X / Vol. 12, No. 24, julio – diciembre de 2018
DOI: http://dx.doi.org/10.21676/23897848.2868

Evaluación del riesgo. Esta actividad tiene por objetivo estimar el nivel de riesgo inherente y determinar cuáles riesgos necesitan tratamiento y la prioridad para su implementación (Calzada y Galarza de León, 2010). El nivel de riesgo dependerá de la combinación de los valores de probabilidad e impacto calculados en la fase anterior. En este proceso se utiliza la herramienta matriz de probabilidad e impacto, que permite clasificar los riesgos por zonas de criticidad (baja, moderada, alta y extrema), con lo cual se pueden priorizar las acciones para el tratamiento.

Tratamiento del riesgo. Esta actividad implica la selección y la implementación de una o varias opciones para modificar el nivel de criticidad de los riesgos. Esta fase se encuentra inmersa en un ciclo de revisión y seguimiento permanente, en el cual la organización identifica los riesgos relevantes y determina los controles que debe implementar para responder ante ellos (Liuksiala, 2012). El desarrollo de esta tarea no se contempla en el alcance del proceso investigativo.

Monitoreo y revisión. Es una actividad esencial para asegurar la adecuada implementación del proceso de gestión del riesgo en las organizaciones. Su relevancia radica en que permite monitorear y documentar el comportamiento de los riesgos, analizando el nivel de eficiencia de las acciones propuestas para eliminar o mitigar su impacto (Mejía y Villanueva, 2014). Esta fase no se contempla en la presente investigación; su ejecución le corresponde al funcionario autorizado por la alta dirección de la entidad.

RESULTADOS

Establecimiento del contexto

En esta primera fase de la metodología se identificaron aquellos factores internos o externos a la caja de compensación que podrían influir en el normal desarrollo de los objetivos de la gestión de aportes. Este análisis se adelantó mediante la técnica de lluvia de ideas formal, tomando como referentes un documento con el análisis del contexto estratégico de la organización, suministrado por la dirección de la entidad, y otro con la caracterización del proceso, suministrado por el jefe del Departamento de Aportes y Subsidio. En la reunión con los funcionarios se les solicitó (1) indicar si estaban de acuerdo con el objetivo del proceso de gestión de aportes, (2) describir situaciones que dificultan el cumplimiento de este, y (3) suministrar información sobre eventos ocurridos durante los últimos dos años y que han afectado el proceso.

A continuación se presenta el resultado del análisis obtenido en construcción colaborativa con los funcionarios de nivel profesional y asistencial del Departamento de Aportes y Subsidio.

Establecimiento del contexto externo:

1. Cambios en la legislación fiscal que inciden en la reducción de aportes parafiscales.
2. Relación con entidades bancarias que afectan la conciliación del recaudo de aportes.
3. Eliminación de aportes parafiscales por mandato legal.
4. Disminución de factores salariales en la liquidación de aportes parafiscales.
5. Relación con proveedores de servicios de telecomunicaciones que afectan la ejecución de las actividades del proceso.
6. Competencia de nuevas empresas que prestan servicios de subsidio familiar.
7. Desmonte de la territorialidad de operaciones de la caja.
8. La obligatoriedad de cumplimiento de normatividad de los empleadores.
9. Pérdida de credibilidad por baja oportunidad de respuesta ante las partes interesadas.
10. Desactualización de la infraestructura de hardware y software.
11. Sanciones por incumplimientos con entes de control.

Establecimiento del contexto interno:

1. Desconocimiento por parte de los funcionarios de la normatividad, las políticas y los lineamientos generales propios del proceso de gestión de aportes.

Clío América / ISSN 1909-941X / Vol. 12, No. 24, julio – diciembre de 2018
DOI: http://dx.doi.org/10.21676/23897848.2868

2. Inadecuada planificación e implementación de requisitos nuevos asociados al proceso.
3. Perfiles de empleados desactualizados y estrechos tiempos de inducción o entrenamiento del personal nuevo.
4. Deficiente motivación laboral debido a la inequidad en la distribución de los recursos y programas de bienestar social.
5. Extemporaneidad en el registro de empresas y trabajadores.
6. Tramitación de solicitudes de afiliaciones de empresas inexistentes o con documentación adulterada o falsificada.
7. Vulnerabilidades de seguridad de los sistemas de información y/o bases de datos asociados al proceso.
8. La captura de datos de las solicitudes de afiliación de empresas y empleados se realiza de forma manual.
9. Escasa cobertura y periodicidad en el fomento de la cultura de administración y prevención de riesgos.
10. Inadecuado espacio físico e inmobiliario para la atención a los afiliados.
11. Falta de acompañamiento y actualización legal para la aplicación de la normatividad del subsidio familiar.

Con base en los factores definidos en la sección anterior, y continuando con la técnica de lluvia de ideas formal, fue posible identificar de forma sistemática las principales causas concretadas de los riesgos del proceso de gestión de aportes. Las 35 causas que se pudieron identificar son:

1. Falta de acompañamiento y actualización legal para la aplicación de la normatividad del subsidio familiar.
2. Deficiente adaptación de las plataformas informáticas que soportan el proceso de gestión de aportes ante los cambios normativos.
3. Falta de aplicación de los controles establecidos para el procedimiento de registro de empresas y trabajadores.
4. Falta de oportunidad en la atención de las solicitudes de afiliación de empresas y trabajadores que se reciben por correo electrónico.
5. Omisión de la normatividad asociada al proceso por parte de los funcionarios.
6. Falencias en los controles establecidos para prevenir o evitar el registro de empresas inexistentes.
7. Ausencia de acuerdos de confidencialidad de la información firmados por los funcionarios del proceso.
8. Desarticulación de la base de datos de la entidad con el sistema de la Cámara de Comercio.
9. Suplantación de empleados y beneficiarios.
10. Alteración y/o modificación de documentos.
11. Falta de capacitación al personal en temas normativos del proceso.
12. Ausencia de mecanismos tecnológicos para la captura automática de datos de las solicitudes de afiliación de empresas y empleados.
13. Controles manuales susceptibles de alteración o modificación.
14. Registro extemporáneo en el aplicativo de los aportes recibidos por PILA, bancos y caja por parte de los funcionarios.
15. Reporte incompleto de planillas de pago por parte del operador, lo que retrasa la conciliación y ocasiona que los empleados y beneficiarios no reciban el subsidio.
16. Generación de diferencias entre los valores de recaudo reportados por el banco en los archivos planos y las planillas de información del operador.
17. Ausencia de sistemas de información que les permitan a los funcionarios generar reportes confiables de empresas omisas e inexactas.
18. Controles manuales susceptibles de alteración o modificación.
19. Direccionamiento de la información del proceso a favor o en contra de terceros.
20. Ausencia de cultura de legalidad de las empresas.
21. Falta de aplicación de controles para el seguimiento e identificación de los pagos efectuados por PILA de las empresas no afiliadas o no identificadas.

Clío América / ISSN 1909-941X / Vol. 12, No. 24, julio – diciembre de 2018
DOI: http://dx.doi.org/10.21676/23897848.2868

22. Desconocimiento de las empresas respecto a los trámites de registro y afiliación a la caja.
23. Demora en la entrega de novedades por parte de las empresas para la afiliación.
24. Criterios de auditoría inapropiados para la verificación de la liquidación de los aportes parafiscales efectuados por las empresas.
25. Sustracción, alteración, manipulación y/o pérdida de informes de auditoría para favorecer a terceros.
26. Sobrecarga de trabajo de los funcionarios, que impide el desarrollo de auditorías.
27. Falta de controles de auditoría a empleadores para determinar eventuales inexactitudes en pagos de aportes por menor valor del real.
28. Inexactitudes en pagos de aportes por menor valor del real.
29. Equipos de cómputo con interfaz de puertos USB desbloqueados que facilitan la extracción de información confidencial.
30. Cambios en la legislación fiscal que inciden en la reducción de aportes parafiscales.
31. Personal inadecuadamente capacitado y concientizado en buenas prácticas de seguridad de la información.
32. Desconocimiento de las políticas y procedimientos de seguridad por parte de los funcionarios del proceso.
33. Insuficiencia en el aseguramiento de las bases de datos utilizadas en el proceso de gestión de aportes.
34. Reducción de los aportes parafiscales por reducción de nóminas en las empresas.
35. Desmonte de la territorialidad de operaciones de la caja.

Identificación del riesgo

Esta segunda fase de la metodología se realizó tomando como referente las causas de riesgos identificadas en la sección anterior, las cuales se organizaron en un documento formal que se suministró a cada funcionario. Mediante la técnica de lluvia de ideas se señalaron 11 riesgos subyacentes a las actividades propias del proceso de gestión de aporte, asociados a aquellos eventos o situaciones que podrían entorpecer el normal desarrollo de los objetivos de este.

En la tabla 3 se presenta la descripción de los riesgos identificados. La primera columna contiene el identificador de la causa asociada a cada riesgo, la segunda columna representa el identificador del riesgo, en la tercera se presenta la descripción del riesgo, y en la cuarta se relacionan las consecuencias o el impacto esperado con la materialización del riesgo.

Tabla 3. Identificación de riesgos del proceso de gestión de aportes

Causas de riesgo	N.º	Riesgo	Consecuencias o impactos
[1] [2] [3]	R1	Incumplimiento en la planificación e implementación de requisitos legales asociados al proceso de gestión de aportes	Investigaciones, sanciones disciplinarias y fiscales
[4] [5] [12] [13] [14]	R2	Retrasos o incumplimientos en la atención de las solicitudes de afiliación de empresas y trabajadores que se reciben por medio de correo electrónico	Reprocesos y desgaste administrativo, afiliación tardía de empresas y empleados, sanciones y demandas
[7] [9] [10] [11]	R3	Fraude en la asignación de subsidios a trabajadores y beneficiarios que no cumplen con los requisitos legales	Investigaciones, pérdida de recursos económicos, estados financieros incorrectos

Clío América / ISSN 1909-941X / Vol. 12, No. 24, julio – diciembre de 2018
DOI: http://dx.doi.org/10.21676/23897848.2868

[18] [19] [20] [21]	R4	Detrimento patrimonial por evasión, elusión y morosidad en el pago de las obligaciones parafiscales	Investigaciones, sanciones disciplinarias y fiscales. Pérdida de imagen y credibilidad
[6] [15] [16] [17] [22] [23] [24]	R5	Incumplimiento en la prestación legal del subsidio familiar por parte de los funcionarios del proceso de gestión de aportes	Investigaciones, sanciones disciplinarias y fiscales. Pérdida de imagen, credibilidad y confianza. Incumplimiento de metas
[25] [26] [27] [28] [29]	R6	Incumplimiento en la ejecución del programa anual de auditorías	Investigaciones, demandas, sanciones disciplinarias y fiscales. Pérdida de imagen, credibilidad y confianza, aprovechamiento de los recursos de forma oportuna
[30] [34] [35]	R7	Pérdidas económicas que disminuyen el monto dinerario del subsidio familiar	Investigaciones, demandas, sanciones disciplinarias y fiscales. Pérdida de imagen, credibilidad y confianza
[8] [29]	R8	Fuga de información	Pérdida de imagen, credibilidad y confianza. Afectación de las dimensiones de seguridad de la información (confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad)
[31] [32] [33]	R9	Pérdida de la información	Pérdida de imagen y credibilidad. Afectación dimensiones de seguridad de la información

Fuente: elaboración propia basada en DAFP (2014).

Análisis del riesgo

Esta fase se realizó haciendo uso de la técnica matriz de consecuencia/probabilidad, con la participación del jefe del Departamento de Aportes (e), quien mediante criterio experto determinó los valores de probabilidad y consecuencia (impacto) para cada riesgo. En la tabla 4 se presenta el resultado del análisis efectuado. La primera columna representa el código asignado a cada riesgo, seguido en la segunda columna del valor de probabilidad de ocurrencia de cada riesgo, para el cual se utilizaron criterios de factibilidad que analizan la presencia de factores internos y externos que pueden propiciar el riesgo. En la tercera columna se determina el nivel de impacto esperado ante la materialización del riesgo.

Tabla 4. Análisis de riesgos (probabilidad/consecuencia)

Código Riesgo	Probabilidad de ocurrencia	Impacto
R1	Posible (3)	Mayor (4)
R2	Posible (3)	Moderado (3)

Clío América / ISSN 1909-941X / Vol. 12, No. 24, julio – diciembre de 2018
DOI: http://dx.doi.org/10.21676/23897848.2868

R3	Improbable (2)	Mayor (4)
R4	Posible (3)	Mayor (4)
R5	Improbable (2)	Mayor (4)
R6	Improbable (2)	Moderado (3)
R7	Rara vez (1)	Catastrófico (5)
R8	Casi seguro (5)	Mayor (4)
R9	Casi seguro (5)	Catastrófico (5)

Fuente: elaboración propia basada en DAFP (2014).

Evaluación del riesgo

Esta fase de la metodología contempló la evaluación del nivel de riesgo inherente al proceso de gestión de aportes, con independencia de los controles dispuestos por la organización. Para la valoración se utilizó una medición semicuantitativa, en la cual se determinó la probabilidad de ocurrencia y el impacto de cada riesgo de acuerdo con una escala descriptiva. La calificación del riesgo se obtuvo a partir de la combinación de los valores de probabilidad e impacto, como se observa en la figura 2.

Figura 2. Mapa de riesgo inherente al proceso de gestión de aportes

probabilidad de ocurrencia						
	Casi seguro 5	5	10	15	20 **(r8)**	25 **(r9)**
	Probable 4	4	8	12	16	20
	Posible 3	3	6	9 **(r2)**	12 **(r1,r4)**	15
	Improbable 2	2	4	6 **(r6)**	8 **(r3,r5)**	10
	Rara vez 1	1	2	3	4	5 **(r7)**
		Insignificante 1	Menor 2	Moderado 3	Mayor 4	Catastrófico 5
		impacto				

SEVERIDAD DEL RIESGO		
CONVENCIÓN	CRITERIOS Y PARÁMETROS	
	Catastrófico	16 - 25
	Mayor	**10 - 15**
	Moderado	**6 - 9**
	Menor	**4 - 5**
	Insignificante	**0 - 3**

Fuente: elaboración propia.

De acuerdo con lo anterior, fue posible agrupar los riesgos en cinco zonas de criticidad:

1. **Catastrófica**. En esta zona se ubican los riesgos críticos para la organización: R8 y R9. De no establecerse medidas de control que mitiguen su impacto, podrían afectar el cumplimiento de los objetivos del proceso.
2. **Mayor**. En esta zona se ubican los riesgos importantes R1 y R4, que en conjunto representan el 22 % de los riesgos valorados en su estado inicial.
3. **Moderada.** En esta zona se ubican los riesgos de importancia media: R2, R3, R5 y R6.
4. **Menor:** Esta zona contiene un único riesgo: R7.
5. **Insignificante:** No existen riesgos para esta zona.

Los resultados obtenidos en la evaluación del riesgo inherente a la gestión de aportes de la caja de compensación familiar Cf indican que, de los nueve riesgos identificados, el 88,8 % se encuentran por encima del nivel de tolerancia, considerados por su naturaleza riesgos críticos e importantes; y el 11,2 % restante está dentro del límite de tolerancia, bajo un nivel moderado. En función de la ubicación de los riesgos en la matriz se logró determinar que los más críticos corresponden a: R8 (pérdida de información) y R9 (afectación de la integridad de los datos del proceso).

Este panorama evidenció una alta exposición a riesgos de origen tecnológico en la organización,

Clío América / ISSN 1909-941X / Vol. 12, No. 24, julio – diciembre de 2018
DOI: http://dx.doi.org/10.21676/23897848.2868

derivados de una inadecuada capacitación y concientización de los funcionarios en políticas y estándares de seguridad de la información, la ausencia de mecanismos de seguridad idóneos para salvaguardar datos personales sensibles y reservados de usuarios y clientes corporativos, el desarrollo de actividades en equipos de cómputo con un software de protección desactualizado, y la ausencia de acuerdos de confidencialidad debidamente firmados por los funcionarios del proceso. Por tanto, de no realizarse seguimiento y tratamiento oportuno a estos riesgos, se podría ver comprometida alguna de las dimensiones de la seguridad de la información (esto corresponde a la confidencialidad, la integridad, la disponibilidad, la trazabilidad y la autenticidad).

DISCUSIÓN

Lalonde y Boiral (2012) consideran que la administración del riesgo constituye en la actualidad un reto estratégico para las organizaciones debido a que el riesgo está en permanentemente evolución y se adapta a las complejas y diversas dinámicas del entorno. Este desafío ha sido asumido por la caja de compensación familiar Cf de forma responsable al establecer una política de gestión del riesgo y una metodología para su instrumentalización. Autores como Florea y Florea (2016) afirman que "la gestión del riesgo es un elemento fundamental del gobierno corporativo y aporta muchos beneficios como resultado de su enfoque estructurado, coherente y coordinado" (p. 77).

La aplicación de la técnica de lluvia de ideas formal para el levantamiento de los riesgos inherentes al proceso se fundamentó en el análisis del contexto estratégico de la caja de compensación, entrevistas a funcionarios y el documento de caracterización del proceso de gestión de aportes y procedimientos asociados. Estas actividades desarrolladas coinciden con los expuesto en Velásquez, Velásquez, Velásquez y Villa (2017), quienes afirman que, para asegurar un adecuado levantamiento de riesgos, es necesario contar con el documento de caracterización de los procesos, el cual debe incluir los objetivos y el alcance asociado; la descripción de los procedimientos relacionados con el proceso objeto de estudio y la bitácora con el registro de incidentes presentados durante los últimos años.

Los resultados de la investigación demuestran que los riesgos más relevantes para el proceso están relacionados con la pérdida de información y la afectación de la integridad de los datos, que por su naturaleza son de origen tecnológico. Según Ramírez y Ortiz (2011), "el daño, interrupción, alteración o falla derivada del uso de las tecnologías de la información puede implicar pérdidas significativas en las organizaciones, pérdidas financieras, multas o acciones legales, afectación de la imagen de una organización y causar inconvenientes a nivel operativo y estratégico" (p. 57).

Este mismo autor plantea que las amenazas de ciberseguridad y los errores informáticos siempre serán factores que obstaculizan el éxito, la reputación y el valor de una organización. De ahí que las pérdidas esperadas ante la violación de datos, el robo de propiedad intelectual o el daño a equipos información sean incalculables, dado que atacan directamente al activo informacional de cualquier entidad.

Lanz (2018) expone que la norma ISO 31000 proporciona a las empresas prácticas de consenso y orientación sobre la mejor manera de gestionar el riesgo. Esto se evidencia en la evaluación, desde el entendido de que la norma propone unos lineamientos generales que las organizaciones deben considerar al implementar el proceso de gestión del riesgo, pero no brinda una metodología descriptiva y precisa que oriente el paso a paso en el desarrollo de las actividades. En este punto cabe considerar que, aunque la filosofía de las normas ISO se fundamenta en el diseño de principios que orientan el "qué hacer", es necesario desarrollar una metodología más descriptiva, que guíe al analista en su implementación.

Como resultado del estudio, se puede afirmar que la evaluación de los riesgos aporta valor a las organizaciones, fortalece sus procesos y mejora el nivel de conocimiento de su entorno. Se espera que esta investigación le permita a la caja de

Clío América / ISSN 1909-941X / Vol. 12, No. 24, julio – diciembre de 2018
DOI: http://dx.doi.org/10.21676/23897848.2868

compensación adoptar una actitud proactiva frente al riesgo y reconocer que la gestión de este no es una tarea excluyente, sino vinculante, que necesita de la experiencia y el conocimiento de todos los funcionarios que hacen parte de la organización.

CONCLUSIÓN

En desarrollo de este trabajo se pudo determinar que para lograr una eficiente administración del riesgo se requiere un conocimiento detallado de la empresa y del contexto interno y externo en el que esta realiza sus operaciones. De ahí que sea importante contemplar la participación de los funcionarios que realizan funciones propias de los procesos sometidos a evaluación, pues son estos quienes disponen de los conocimientos, las habilidades y las destrezas necesarias para la identificación de los riesgos.

Una adecuada aplicación de la norma NTC ISO 31000:2011 contribuye a prevenir o mitigar las pérdidas económicas, de información, reputacionales y otras asociadas a la materialización de eventos adversos que pueden afectar la gestión de aportes de la caja de compensación familiar Cf. Esta norma busca que la entidad adopte una cultura proactiva frente al riesgo y que los funcionarios reconozcan la importancia de gestionar los riesgos inherentes al desarrollo de sus actividades.

La implementación de la metodología de administración del riesgo con base en NTC ISO 31000:2011 se aplicó únicamente para la identificación, el análisis y la evaluación de los riesgos inherentes al proceso de gestión de aportes; por tanto, se recomienda que la caja de compensación familiar Cf continúe con la etapa de evaluación y tratamiento para los riesgos que obtuvieron una calificación por encima del nivel de tolerancia, considerados críticos e importantes, y se efectúe un seguimiento y revisión permanente a aquellos que presentaron una calificación moderada.

Una limitación que se presentó en el desarrollo de la investigación fue la actualización de la norma NTC ISO 31000 en su versión 2018, publicada una vez que el proceso de análisis, identificación y valoración inicial del riesgo se había realizado en la caja de compensación familiar. Esta nueva actualización conservó la estructura del proceso de gestión del riesgo propuesto en la NTC ISO 31000:2011, pero agregó un elemento de documentación y presentación de informes de gestión del riesgo.

Como estudio futuro se propone aplicar la metodología de administración de riesgos bajo un enfoque cuantitativo, que permita estimar la magnitud del impacto de los riesgos en términos económicos. El objetivo de esto es facilitar la toma de decisiones en relación con el costo-beneficio para la organización en el momento de invertir en estrategias para eliminar o controlar los riesgos.

Declaración sobre conflicto de interés
Los autores del presente estudio manifestamos que este trabajo no ha sido financiado por terceros y que durante la ejecución del trabajo o la redacción del manuscrito no han incidido intereses o valores distintos a los que usualmente tiene la investigación.

REFERENCIAS BIBLIOGRÁFICAS

Arias, R. Y., Díaz, R. M. y Vargas, C. J. (2014). *Elaboración de una guía de gestión de riesgos basados en la norma NTC ISO 31000 para el proceso de gestión de incidentes peticiones de servicio del área de mesa de ayuda de empresas de servicios de soportes de tecnología en Colombia* (Tesis de pregrado). Recuperado de http://repository.ucatolica.edu.co/bitstream/10983/1758/1/Trabajo%20de%20Grado%20Especializacion%20Auditoria%20de%20Sistemas.pdf

Calzada, R. y Galarza De León, J. (2010). Características de la gestión de riesgos en las empresas cubanas. *Revista cubana de ciencias informáticas, 4*(3), 1-10. Recuperado de

https://rcci.uci.cu/?journal=rcci&page=article&op=view&path%5B%5D=90&path%5B%5D=109

Castillo, S. C. (2016). *Propuesta metodológica para la identificación de riesgos asociados a la gestión documental* (Tesis de maestría). Recuperado de https://ddd.uab.cat/pub/trerecpro/2017/hdl_2072_272839/TrabajoClaudiaCastilloCorrecto.pdf

Cervantes, I., Hernández, O. y Reyes, J. (2017). *Identificación de riesgos con un enfoque basado en procesos* (Tesis de pregrado). Recuperado de http://tesis.ipn.mx/handle/123456789/20779

Departamento Administrativo de la Función Pública (DAFP). (2014). *Guía para la administración del riesgo* (versión 3). Recuperado de http://www.funcionpublica.gov.co/eva/admon/files/empresas/ZW1wcmVzYV83Ng==/archivos/1486395001_49cd5a628610035d8ed7c899ec810e3c.pdf

Espino, P. M. (2014). *Desarrollo de un modelo de gestión de riesgos según la Norma UNE ISO 31000 para el tratamiento de reclamaciones en edificación* (Tesis doctoral). Recuperado de https://idus.us.es/xmlui/handle/11441/26883

Florea, R. y Florea, R. (2016). Internal Audit and Risk Management. ISO 31000 and ERM Approaches. *Economy Transdisciplinarity Cognition*, *19*(1), 72-77. Recuperado de http://www.ugb.ro/etc/etc2016no1/13_Florea_Radu__Florea_Ramona.PDF

García, K. y Suárez, Y. (2017). *Aplicación de la metodología NTC ISO 31000 para la evaluación de los riesgos generados en el proceso de deudores en la Universidad de la Amazonia* (Tesis de especialización).Universidad de la Amazonía, Florencia, Caquetá, Colombia.

Hinestroza, Y. y González , D. (2018). *Riesgo político en las Cajas de Compensación de Colombia: un estudio cualitativo* (Tesis de maestría).Universidad EAFIT, Medellín, Antioquia, Colombia.

Instituto Colombiano de Normas Técnicas y Certificación (Icontec). (2011). *Gestión del riesgo. Principios directrices*. Recuperado de https://sitios.ces.edu.co/Documentos/NTC-ISO31000_Gestion_del_riesgo.pdf

International Organization for Standardization (ISO). (2009). *ISO 31010:2009 Risk management - Risk assessment techniques.*

Lalonde, C. y Boiral, O. (2012). Managing risks through ISO 31000: A critical analysis. Risk Management. *Palgrave Macmillan Journals*, *14*(4), 272-300. Doi:10.1057/rm.2012.9

Lanz, J. (2018). Enterprise Technology Risk in a New COSO ERM World: Eight Challenges Facing Management. *CPA Journal*, *88*(6), 6-10. Recuperado de https://www.cpajournal.com/2018/06/19/enterprise-technology-risk-in-a-new-coso-erm-world/

Lascano, R., Caro, L. y Arcieri, E. (2008). Aplicación del Estándar Australiano de Administración del Riesgo AS/NZS 4360:1999 en la empresa GECELCA. *Pensamiento y Gestión*, (25), 94-112. Recuperado de http://rcientificas.uninorte.edu.co/index.php/pensamiento/article/view/3206

Lavielle, F. V. (2016). *Desarrollo de gestión de riesgos en contratos de construcción, bajo el estándar ISO 31000, orientado hacia la calidad y la sustentabilidad* (Tesis de pregado). Recuperado de http://repositorio.uchile.cl/bitstream/handle/2250/141778/Desarrollo-de-gestion-de-riesgos-en-contratos-de-construccion-bajo-el-standar-ISO-31000-orientado.pdf?sequence=1

Liuksiala, A. (2012). The use of the risk management standard ISO 31000 in finnish organizations (Tesis de maestría). Recuperado de http://tampub.uta.fi/bitstream/handle/10024/84249/gradu06462.pdf;sequence=1

Mejía, R. (2004). La administración de riesgos empresariales. *Revista Ad-Minister, 1*(5), 74-85. Recuperado de http://publicaciones.eafit.edu.co/index.php/administer/article/view/679/605

Mejía, R. y Villanueva, E. (2014). Metodología para monitorear riesgos estratégicos. *Revista de investigaciones de la Universidad de Quindio, 26*(1), 122-132. Recuperado de http://blade1.uniquindio.edu.co/uniquindio/revistainvestigaciones/adjuntos/pdf/c059_122-132.pdf

Oliver, A. (2015). *Gestión del riesgo (Risk Management ISO 31000). Aplicación práctica en una empresa de seguridad electrónica* (Tesis de maestría). Recuperado de https://rdu.unc.edu.ar/bitstream/handle/11086/2681/Olive%2C%20Antonio.%20Gesti%C3%B3n%20del%20riesgo.pdf?sequence=1&isAllowed=y

Preve, L. (2015). Gestionar riesgos nos permite hacer más negocios. *IEEM Revista de Negocios, 1*(6), 54-55.

Pulido, R. A. (2015). Methodological design for the prevention of risk in production processes. *Revista DYNA, 82*(193), 16-22. Recuperado de http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0012-73532015000500002

Purdy, G. (2010). ISO 31000:2009 setting a new standard for risk management. *Perspective, 30*(6), 881-886. Doi: 10.1111/j.1539-6924.2010.01442.x

Ramírez, C. A. y Ortiz, B. Z. (2011). Gestión de riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. *Ingeniería, 16*(2), 56-66. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=4797252

Rodríguez, T. Y. (2016). *Diseño y formulación de un sistema de gestión de riesgos basados en los lineamientos establecidos por la norma NTC -ISO 31000 versión 2011 para la empresa SIMMA LTDA* (Tesis de pregrado). Recuperado de http://tangara.uis.edu.co/biblioweb/tesis/2016/163435.pdf

Santofimio, C. Y. y Manrique, V. C. (2015). *Técnicas de evaluación del riesgo para determinar la viabilidad del proyecto en la etapa de formulación* (Tesis de especialización). Recuperado de http://bibliotecadigital.usb.edu.co/bitstream/10819/3063/1/Tecnicas_evaluacion_riesgo_santofimio_2015.pdf

Uribe, I. J. (2012). *Propuesta metodológica para la aplicación de la norma ISO 31000:2009 en el sistema de gestión de*

calidad de la Universidad Libre en la sede Bosque Popular para el proceso de servicios generales en el subproceso de mantenimiento (Tesis de especialización). Recuperado de http://repository.unilibre.edu.co/bitstream/handle/10901/9905/MONOGRAFIA.pdf?sequence=1

Valencia, M. G. (2013). *Modelo de gestión de riesgos aplicando el estandar AS/NZS 4360 y la norma ISO 31000:2009 para la gestión administrativa del gobierno autonómo descentralizado de San Miguel de Ibarra* (Tesis de pregrado). Recuperado de http://repositorio.utn.edu.ec/bitstream/123456789/2437/1/02%20ICA%20546%20TESIS.pdf

Velásquez, P., Velásquez, S., Velásquez, M. y Villa, J. (2017). Implementación de la gestión de riesgo en los procesos misionales de la Sección de Dermatología de la Universidad de Antioquia (Medellín, Colombia) siguiendo las directrices de la norma ISO 9001:2015. *Revista Gerencia y Políticas de Salud, 16*(33), 78-101. Recuperado de http://www.redalyc.org/pdf/545/54553416006.pdf

Zapata, S. A. (2015). *Análisis de riesgos por procesos basado en la norma ISO 31000:2009 para el centro comercial premier el Limonar Cali* (Tesis de pregrado). Recuperado de https://red.uao.edu.co/bitstream/10614/8029/1/T06032.pdf