

## CENTRAL DE INVERSIONES S.A. - CISA

### INFORME EJECUTIVO DE EVALUACION DE RIESGOS

#### INTRODUCCIÓN

En cumplimiento al rol de evaluación y seguimiento que tienen la Auditoría Interna, en el marco de la evaluación del Sistema de Control Interno y especialmente en la valoración de riesgos como parte de uno de los componentes del MECI, el equipo de trabajo de la Auditoría Interna realizó la verificación a la definición de controles y acciones de mitigación establecidos por cada uno de los procesos identificados en Central de Inversiones S.A, evaluación realizada entre el 17 y 31 de marzo de 2017.

#### ANTECEDENTES RELACIONADOS CON LA ADMINISTRACIÓN DEL RIESGO.

- a. El Manual Técnico del Modelo Estándar de Control Interno – MECI: 2014, establece dentro de sus tres (3) principios rectores para la implementación del Sistema de Control Interno el principio de **“Autogestión”** el cual indica que al interior de cada Entidad *“... La organización deberá establecer políticas, acciones, métodos, procedimientos y mecanismos de prevención, control, evaluación y mejoramiento continuo que permitan dar cumplimiento a cada uno de estos principios, con el propósito de estructurar un Sistema de Control Interno que permita tener una seguridad razonable en el cumplimiento de sus objetivos”*.<sup>1</sup> (Subrayado fuera del texto)

Así mismo establece en el literal (d) de sus objetivos de Control de Planeación y Gestión entre otros, la implementación de mecanismos que protejan los recursos de la organización, buscando su adecuada administración ante los posibles riesgos que los afecten.

- b. El proceso de Direccionamiento Estratégico de CISA, desarrolló la Circular Normativa 107 “Administración de Riesgo en Central de Inversiones”, la cual indica en el numeral 5° cual es la política adoptada para la entidad así<sup>2</sup>:

#### 5. POLITICAS DE ADMINISTRACIÓN DEL RIESGO

CISA adopta como base metodológica para la identificación, análisis, evaluación y tratamiento de los riesgos operativos y de seguridad de la información, la Norma Técnica Colombiana NTC ISO 31000:2009 “Gestión del Riesgo. Principios y Directrices”.

Conforme a lo estipulado en el decreto 124 de enero de 2016, para la gestión de los riesgos de corrupción de que trata el artículo 73 de la Ley 1474 de 2011 se utilizará la metodología establecida en el documento "Guía para la Gestión del Riesgo de Corrupción" del Departamento Administrativo de la Función Pública.

El Gerente de Planeación debe proponer para aprobación de la Alta Dirección la Política y Objetivos para la Administración del Riesgo, los cuales deben estar alineados con el direccionamiento estratégico de la Organización.

<sup>1</sup> Tomado del Manual Técnico del MECI – 2014, Pág. 13

<sup>2</sup> Tomado de la Circular Normativa 107 Versión 13 del 17 de junio de 2016.

Adicionalmente indica como responsabilidades del Auditor Interno en el marco de la administración de riesgo para CISA las siguientes:

**El Auditor Interno, es responsable de:**

Evaluar periódicamente el cumplimiento de las políticas, su actualización y que estas se estén ejecutando.

Brindar una evaluación objetiva sobre la administración de los riesgos, valorar la efectividad de los controles, realizar seguimiento a las acciones establecidas en los planes de tratamiento y emitir informes periódicos a la presidencia de la entidad o al Comité Asesor de Junta Directiva de auditoría.

Opinar acerca de la suficiencia y pertinencia del Mapa de Riesgos, de las acciones para su tratamiento.

**PROCESOS ANALIZADOS:**

Para cada uno de los 14 procesos identificados en el Mapa de procesos de CISA – versión 7, se verificó que tanto en la Matriz de Riesgos Operativos como la de Riesgos de Corrupción, actualizados en el mes de diciembre de 2016, evaluando que se hallan identificado (los) control(es) para su tratamiento, las acciones de mitigación asociadas que permitan evidenciar su efectividad frente a los riesgos, en cumplimiento de la política establecida en la Circular Normativa 107, así mismo se solicitó a cada proceso se identificaran las evidencias tanto documentales como electrónicas frente a la cual se evaluara la efectividad del control.

2

TABLA 1 – Procesos Evaluados

No.	PROCESO	RIESGOS OPERATIVOS	RIESGOS DE CORRUPCIÓN
1	ADMINISTRATIVA Y SUMINISTROS	4	3
2	COMUNICACIÓN CORPORATIVA	4	0
3	DIRECCIONAMIENTO ESTRATÉGICO	6	0
4	FINANCIERA Y CONTABLE	2	2
5	GESTION DEL TALENTO HUMANO	2	5
6	GESTION INTEGRAL DE ACTIVOS - CARTERA	3	6
	GESTION INTEGRAL DE ACTIVOS - INMUEBLES	6	9
7	GESTION INTEGRAL DE SERVICIOS	2	0
8	GESTION JURÍDICA DEL NEGOCIO	4	4
9	INFRAESTRUCTURA TECNOLÓGICA	6	6
10	LEGAL	5	2
11	MEJORAMIENTO CONTINUO	3	2
12	SERVICIO INTEGRAL AL USUARIO	1	4

13	SOLUCIONES PARA EL ESTADO	2	0
14	AUDITORIA INTERNA	2	3
<b>TOTALES</b>		<b>52</b>	<b>46</b>

Fuente: Planeación – actualización Dic/ 2016

De las matrices entregadas por el área de Planeación se identificaron 52 riesgos operativos y 46 de corrupción, los cuales fueron analizados con cada líder de proceso en mesas de trabajo con el equipo de auditoría, resaltando la importancia de tener un Mapa de Riesgos que soporte al proceso en su exposición a posibles eventos de riesgos y la manera de mitigar su materialización.

### OBSERVACIONES GENERALES:

Se analizaron las matrices entregadas por el proceso de Planeación tanto para los riesgos operativos como de corrupción, evidenciando lo siguiente:

- a. De acuerdo con lo establecido en la CN 107 para hacer la actualización de los riesgos se efectuó una revisión anual, la cual se realizó en los meses de octubre a diciembre de 2016, con los formatos de Anexo 1 – Levantamiento de Riesgos Operativos y Anexo 2 – Levantamiento de Riesgos de Corrupción por cada proceso del SIG<sup>3</sup>, sobre la cual se realizó la verificación objeto de este informe y que fue remitida por el proceso de planeación.
- b. La política y los procedimientos para la gestión de riesgos establecida en la Circular Normativa 107, debe ser alienada y ajustada con los parámetros normativos establecidos por la oficina de Transparencia de la Presidencia de la República y el Departamento Administrativo de la Función Pública- DAFP.
- c. Según lo establecido en el numeral 6.1 “Procedimiento para la Gestión de Riesgos” de la CN 107, los procesos deben realizar la actualización de los riesgos no solo en los formatos mencionados, si no en la herramienta para la administración del SIG - módulo de riesgos, actividad que no están realizando los procesos, toda vez que la información publicada en la herramienta difiere de la entregada por el área de planeación y la cual fue actualizada en el mes de diciembre de 2016.
- d. Dado los cambios de algunos líderes de proceso y sus equipos, se realizaron ajustes tanto en la inclusión, solicitud de retiro y redacción de algunos riesgos, así como en la definición de los controles y acciones de tratamiento, como se evidencia a continuación:  
..

3

<sup>3</sup> Sistema Integrado de Gestión

TABLA 2- Inclusión y Exclusión de Riesgos

No.	PROCESO	Riesgos Operativos		Riesgos de Corrupción	
		Nuevos	Retiro	Nuevos	Retiro
1	ADMINISTRATIVA Y SUMINISTROS			1	
2	GESTION DEL TALENTO HUMANO	1	1	2	2
3	GESTION INTEGRAL DE ACTIVOS - INMUEBLE	1	1	1	3
4	LEGAL			1	1
<b>TOTALES</b>		<b>2</b>	<b>2</b>	<b>5</b>	<b>6</b>

Fuente: Entrevista con los procesos Marzo/2017

Gráfica 1 – Cambios en la definición de los Riesgos



4

En la gráfica 1 se evidencia que el 28% de los procesos realizó actualización, modificación o solicitó el retiro de los riesgos identificados, situación que de acuerdo con las mesas de trabajo realizadas corresponde a que el actual responsable del proceso no fue quien realizó la identificación.

Se evidenció en las mesas de trabajo que los controles identificados presentan debilidades toda vez que de acuerdo con lo establecido en la guía para la administración de riesgos, versión 2, publicada por el DAFP<sup>4</sup>, estos deben tener en cuenta como aspectos claves lo siguiente:

<sup>4</sup> DAFP: Departamento Administrativo de la Función Pública

## Análisis y Evaluación de Controles

### Aspectos Clave

1. Determinar la naturaleza del control:
  - ✓ **Preventivo:** Evitan que un evento suceda. Ejemplo: login y password en un sistema de información previene (teóricamente) que personas no autorizadas puedan ingresar al mismo.
  - ✓ **Detectivo:** Permiten registrar un evento después de que ha sucedido. Ejemplo: registro de las entradas de todas las actividades llevadas a cabo en el sistema de información, traza de los registros realizados, de las personas que ingresaron, entre otros.
  - ✓ **Correctivo:** No prevén que un evento suceda, pero permiten enfrentar la situación una vez se ha presentado. Ejemplo: pólizas de seguro y otros mecanismos de recuperación de negocio o respaldo, que permiten volver a recuperar las operaciones.
2. **Determinar si los controles están documentados:** Aspecto que permite conocer cómo se lleva a cabo el control, quién es el responsable de su ejecución y cuál es la periodicidad para su ejecución, lo cual determinará las evidencias que van a respaldar la ejecución del mismo.
3. **Establecer si el control es:**
  - ✓ **Automático:** Utilizan herramientas tecnológicas como sistemas de información o software que permiten incluir contraseñas de acceso, o con controles de seguimiento a aprobaciones o ejecuciones que se realizan a través de éste, generación de reportes o indicadores, sistemas de seguridad con scanner, sistemas de grabación, entre otros.
  - ✓ **Manual:** Políticas de operación aplicables, autorizaciones a través de firmas o confirmaciones vía correo electrónico, archivos físicos, consecutivos, listas de chequeo, controles de seguridad con personal especializado, entre otros.
4. **Determinar si los controles se están aplicando en la actualidad y si han sido efectivos para minimizar el riesgo.**

5

No obstante en las matrices como fuente de análisis, se describen controles sin tener en cuenta lo anteriormente planteado, identificando controles tales como:

- “Circular normativa xxx”
- “Manual de Contratación”
- “Envío de Reportes”
- “Comité Técnico institucional de Desarrollo Administrativo”
- “Indicadores”, entre otros

Controles que no permiten establecer la acción puntual que minimice la exposición al riesgo y no es posible su verificación al no tener un soporte o evidencia de su ejecución, situación que fue atendida por los líderes de los procesos, realizando las actualizaciones y ajustes correspondientes, para su posterior formalización ante el área de Planeación como responsable de la administración del Riesgo en CISA.

e. En el desarrollo de las mesas de trabajo realizadas con los procesos, se identificaron los siguientes riesgos como de mayor incidencia al interior de CISA:

1. Riesgos de Corrupción:
  - ✓ Manejo de Información privilegiada
  - ✓ Manipulación de la Información
  - ✓ Errores en la gestión de la información
  - ✓ Gestión de Recursos

## 2. Riesgos Operativos:

- ✓ Incumplimiento de actividades programadas
- ✓ Demoras en la prestación de los servicios
- ✓ Fallas en la definición de los productos o servicios planteados
- ✓ Inexactitud en el cargue de información

### RIESGOS MATERIALIZADOS

Se evidenció la materialización de dos riesgos operativos y dos de corrupción, los cuales fueron registrados a través de auditorías internas y externas realizadas, lo que evidencia falta de control y seguimiento por parte de los líderes de los procesos y de la oficina de planeación como responsable de la Administración de Riesgos en CISA.

**Proceso:** Servicio Integral al Usuario

**Riesgo:** Respuesta no oportuna o inexacta de PQR'S

**Registro de la Materialización:** Auditoría Interna de Gestión

**Tratamiento:** Se suscribió plan de mejoramiento del proceso en el cual se deben fortalecer los controles relacionados con la divulgación de los procedimientos y tiempos de respuesta.

**Proceso:** Administrativa y Suministros

**Riesgo:** Programa de Gestión Documental desalineado con la política del AGN

**Registro de la Materialización:** Auditoría Externa del AGN

**Tratamiento:** Se suscribió plan de mejoramiento con el AGN, proceso en el cual se deben fortalecer los controles relacionados con la implementación de las herramientas que soportan el Programa de Gestión Documental.

**Proceso:** Gestión de Activos - Cartera

**Riesgo:** Reporte inexacto de información financiera de clientes a centrales de riesgo.

**Registro de la Materialización:** Auditoría Interna de Calidad.

**Tratamiento:** Ajustar el archivo base de trasmisión de la información a las centrales de riesgo.

**Proceso:** Gestión de Activos - Inmuebles

**Riesgo:** Divulgación de información sensible de las ofertas en los procesos de puja o subasta para favorecer a terceros"

**Registro de la Materialización:** Auditoría Interna de Gestión

**Tratamiento:** Sin información por parte de la Alta Dirección.

### RECOMENDACIONES:

1. Realizar capacitación al interior de los procesos frente a la Gestión de Riesgos
2. Ajustar la Circular Normativa en los términos establecidos por la normatividad legal vigente que le aplique así mismo determinar la periodicidad de revisión de los riesgos y sus controles asociados.
3. Generar cultura de control al interior de los procesos, basada en la identificación y reporte de posibles eventos de riesgos.

4. Por tratarse de un tema transversal en la entidad la citada política y sus actualizaciones deben ser responsabilidad de todos los líderes de proceso.

**ANEXOS:**

1. Matriz de riesgos operativos con ajustes
2. Matriz de riesgos de corrupción con ajustes.

Bogotá, 17 de abril de 2017

ORIGINAL FIRMADO  
**ELKIN ORLANDO ÁNGEL MUÑOZ**  
AUDITOR INTERNO

Elaboró: Mauren Andrea González S. – Auditor  
Aprobó: Elkin Orlando Angel Muñoz – Auditor Interno

7

