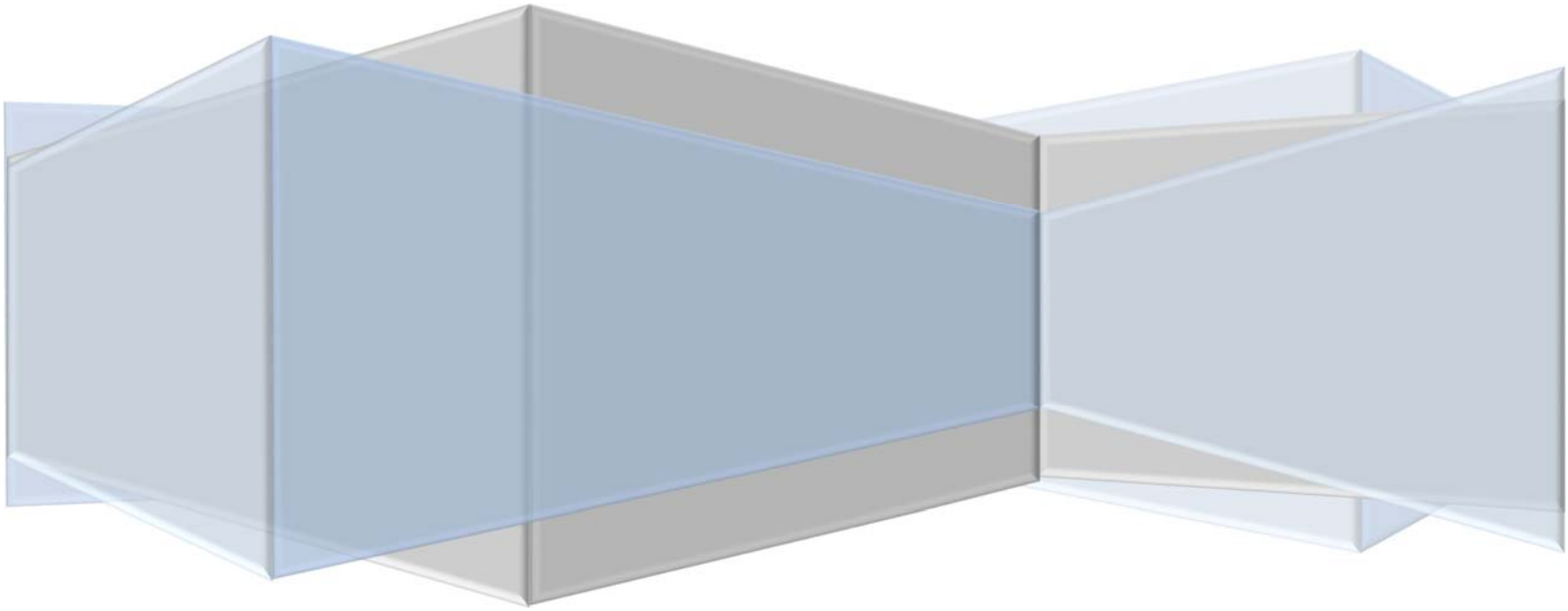
Operadora de Pensiones Complementarias de la CCSS

POLÍTICA DE RIESGO OPERATIVO OPC-CCSS



El riesgo operativo es la cuantificación de las posibles pérdidas ocasionadas por errores o fallas de producto ya sea por factores humanos, sistemas o procedimientos.
Para lo cual las Operadoras, deberá de crear una reserva económica para la cobertura de los posibles eventos que se presenten.

Objetivo General

- Administrar los riesgos operativos de manera que estos mantengan los niveles aceptables de riesgo aprobados por la Junta Directiva.

Objetivo Específicos

- Identificar, evaluar, medir, monitorear y controlar los eventos de riesgos operativos de una forma preventiva, utilizando modelos cualitativos para obtener los niveles de riesgos en que se encuentre la OPC-CCSS.
- Identificar, evaluar, medir, monitorear y controlar los eventos de riesgo operativos de una forma posterior, basado en la metodología propuesta por Basilea II.
- Identificar, evaluar, medir, monitorear y controlar los eventos de riesgo legal de la OPC-CCSS.
- Evaluar los procedimientos, instructivos, manuales de las diferentes áreas, con el fin de detectar posibles errores en la ejecución.
- Crear planes de mitigación de riesgo operativo, cuando los niveles de riesgo son mayores a los aprobados.

Conceptos de riesgo operativo

La Operadora de Pensiones Complementaria de la CCSS define los siguientes factores de riesgos para clasificar todo acontecimiento que afecte los objetivos pactados con el cliente tanto interno como externo:

Incidente de Riesgo Operativo

Es la posibilidad de obtener pérdidas financieras relacionadas con el diseño inapropiado de los procesos críticos, políticas y procedimientos inadecuados o inexistentes; asociadas a la negligencia, error humano, sabotaje, fraude, robo, paralizaciones, apropiación de información sensible, lavado de dinero, inapropiadas relaciones interpersonales y ambiente laboral desfavorable, falta de especificaciones claras en los términos de contratación del personal, entre otros factores, que puedan tener como consecuencia la ejecución deficiente de las operaciones y servicios, o la suspensión de los mismos.

Se pueden también incluir pérdidas asociadas con insuficiencia de personal o personal con destrezas, entrenamiento y capacitación inadecuada o prácticas débiles de contratación, así como los riesgos derivados de fallas en la seguridad y continuidad operativa de los sistemas TI.

Evento de Riesgo operativo

Un evento de riesgo operativo es la posibilidad de obtener pérdidas financieras por errores ya sea por factores humanos, sistemas o procedimientos, pero sin generar un impacto significativo (económico, legal, normativo, entre otros) a los servicios brindados por la OPC CCSS.

Incidente de Seguridad de la Información

Un incidente de seguridad de la información es indicado por un único incidente o una serie de eventos indeseados o inesperados que tienen una probabilidad significativa de paralizar las operaciones y servicios que brinda la Operadora; además de amenazar la información crítica

de la organización, con posibles fugas de información que comprometen la confidencialidad, integridad, disponibilidad y auditabilidad de la organización.

Evento de seguridad de la información

Es una violación o una amenaza inminente a lo declarado en el documento **7PO06 Política General de Seguridad de la Información** y sus procedimientos e instructivos derivados, los mismos tienen un menor impacto que los incidentes.

La gestión del riesgo operativo.

La OPC-CCSS debe identificar, evaluar, medir, monitorear, controlar y documentar los riesgos operativos a los que se encuentra expuesta, los cuales se deberán hacer de la siguiente manera:

Identificación

La identificación efectiva del riesgo considera tanto los eventos internos, como externos que podrían afectar adversamente el logro de los objetivos estratégicos de la OPC-CCSS.

Evaluación

Para todos los riesgos operativos que han sido identificados, la OPC-CCSS debe decidir si usa procedimientos apropiados de control o mitigación de los riesgos o bien asumir las posibles pérdidas en caso de que ocurran.

Todos los riesgos deberán ser evaluados por probabilidad de ocurrencia e impacto, la medición de la vulnerabilidad de la entidad a este riesgo. Los riesgos pueden ser aceptados, mitigados o evitados de una manera consistente con la estrategia de la OPC-CCSS.

Medición

La OPC-CCSS deberá estimar el riesgo inherente y residual en todas sus actividades, productos, áreas particulares o conjuntos de actividades, portafolios, usando técnicas cualitativas basadas en análisis de la Área de Riesgos de la OPC-CCSS.

Monitoreo

Un proceso efectivo de monitoreo es esencial para una gestión adecuada del riesgo operativo. Un monitoreo regular de las actividades puede ofrecer la ventaja de detectar y corregir rápidamente deficiencias en las políticas, procesos y procedimientos de gestión del riesgo operativo. El proceso fomenta la identificación temprana de cambios materiales en el perfil de riesgo, así como la aparición de nuevos riesgos. El alcance de las actividades de monitoreo incluye todos los aspectos de la gestión del riesgo operativo en un ciclo de vida consistente, con la naturaleza de sus riesgos, el volumen, tamaño y complejidad de las operaciones.

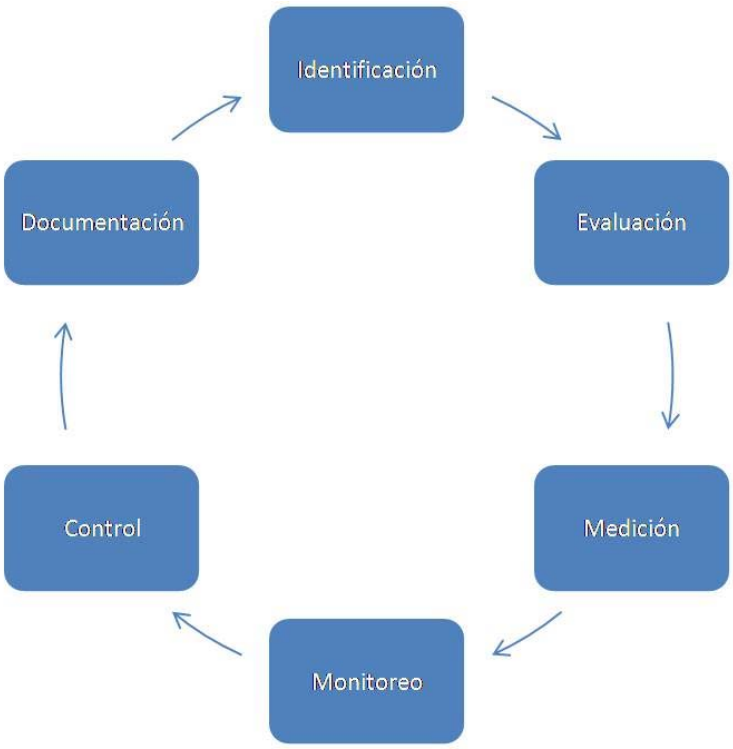
Control

Una vez de identificado y medidos los riesgos a los que está expuesta la OPC-CCSS, está deberá concentrarse en la calidad de la estructura de control interno. El control del riesgo operativo puede ser conducido como una parte integral de las operaciones; a través de evaluaciones periódicas separadas o ambos. Todas las deficiencias o desviaciones deben ser reportadas a la Gerencia.

Documentación

Debe existir un reporte regular de la información pertinente a la Junta Directiva, Gerencia General, Direcciones, al personal y a partes externas interesadas. El reporte puede incluir información interna y externa, así como información financiera y operativa.

El diagrama a continuación muestra la gestión del riesgo operativo expuesta anteriormente:



Clasificación de riesgos operativos de la OPC-CCSS.

La Operadora de Pensiones Complementaria de la CCSS define la siguiente estructura de riesgos:

a. Fraude interno: pérdidas ocasionadas por actos con intención de una defraudación, apropiación indebida o actos fraudulentos contra la ley o la política de la Operadora que involucren al menos a una parte interna.
b. Fraude externo: pérdidas ocasionadas por actos con intención de una defraudación, apropiación indebida o actos fraudulentos, por parte de agentes externos a la Operadora.
c. Prácticas en el lugar de trabajo y seguridad: pérdidas ocasionadas por actos no consistentes con las leyes y contratos de trabajo, salud y seguridad; reclamos por pago de daños y perjuicios personales o por eventos de discriminación religiosa, racial o situaciones fortuitas.

d. Clientes, productos y prácticas del negocio: pérdidas ocasionadas por fallas no intencionadas o negligencia en el cumplimiento con obligaciones profesionales sobre clientes específicos o derivadas de la naturaleza o diseño de un producto.
e. Daño a activo físico: pérdidas ocasionadas por afectaciones o daño a activos físicos debido a desastres naturales u otros eventos.
f. Interrupción de negocios o fallas en sistemas: pérdidas ocasionadas por interrupción del negocio o fallas en sistemas electrónicos, medios digitales, informáticos, telecomunicaciones.
g. Ejecución, entrega y manejo de procesos: pérdida por proceso fallido de transacciones, por procedimientos administrativos, por fallas de negociación con contrapartes, proveedores y multas o sanciones.

Estructura de Riesgos Operativos de la OPC-CCSS

Gestión Preventiva

Para gestionar el riesgo operativo de una forma preventiva el Área de Riesgos se basa en las directrices generales de la Contraloría General de la República mediante la Resolución R-CO-64-2005 del 1° de julio de 2005, que constituye el marco general de referencia para el Sistema Específico de Valoración del Riesgo Institucional (SEVRI).

En atención a lo anterior, la OPC-CCSS concreta este tema mediante un enfoque integral y crea un sistema de valoración integral del riesgo. Este sistema es una herramienta útil para el mejoramiento constante de los servicios y la detección oportuna de las desviaciones de los objetivos encomendados.

Gestión sobre la materialización de los riesgos

Para gestionar el riesgo operativo cuando se haya materializado los eventos de riesgo el Área de Riesgos utilizará las técnicas de modelos avanzados (AMA), sugeridas por el Comité de Basilea como, las más explicativas en cuanto sus indicadores. La OPC-CCSS identifica las

actividades críticas, generadoras de potenciales pérdidas que ocurren dentro de determinados eventos de riesgo, que podrían tener ocurrencia a lo largo de cada uno de esos procesos sustantivos, para estructurar mapas de riesgo institucionales.

Para la obtención de los datos se utilizarán las matrices de: producción, toma de decisiones y apoyos.

Gestión del Riesgo Legal

Para gestionar el riesgo legal la OPC-CCSS deberá realizar lo indicado en el artículo 17 del Reglamento de Inversiones, el cual expone lo siguiente:

> *"Las entidades reguladas deberán valorar como mínimo:*
> *a) Las políticas y procedimientos en busca de una adecuada instrumentación de los convenios y contratos en los que participen, delimitando claramente sus derechos y obligaciones contractuales.*
>
> *b) Determinar las consecuencias legales producto de la actividad de la entidad en función de la administración de ahorro público según los términos que establecen la legislación aplicable.*
>
> *c) Difundir ampliamente entre los funcionarios y empleados, las disposiciones legales y administrativas aplicables a sus operaciones, así como las implicaciones que conllevan su ejercicio.*
>
> *d) Establecer las acciones jurídicas y administrativas pertinentes que permitan tutelar el riesgo de contraparte, ante el evento de incumplimiento de un emisor, de modo que se logre la máxima recuperabilidad de la inversión mediante la ejecución de colaterales u otras garantías.***"**

Evaluación de procedimientos, instructivos y manuales OPC-CCSS

Para gestionar la evaluación de los diferentes procedimientos, instructivos y manuales la OPC-CCSS deberá utilizar lo indicado en las Norma ISO 9001:2015 específicamente el Capítulo 9 Evaluación del desempeño, punto 9.2 Auditoría interna.

Mitigación de Riesgos

Para todos los eventos de riesgo que se encuentren sobre los niveles mayores a los aceptados, se deben gestionar los planes de saneamiento por parte de las jefaturas encargadas, con el

fin de minimizarlos. Si al realizar esta gestión, la exposición del riesgo es mayor al nivel aceptable se deberá presentar ante la Gerencia General un informe detallado, justificando porque no se puede disminuir el riesgo y las posibles formas de provisionarlo.

El diagrama a continuación muestra la estructura de riesgos operativos de la OPC-CCSS.

Niveles de tolerancia al Riesgo Operativo

Tolerancia aceptable para procesos de la operadora

Mediante el acuerdo 3° de la sesión 759 realizada el miércoles 19 de noviembre de 2010 por la Junta Directiva, el cual indica lo siguiente:

> *Acuerdo 3°*
> *Aprobar el cambio en el límite máximo de riesgo operativo con el transitorio propuesto de 10% para el 2010 hasta el 3% en el año 2014 con base en la justificación técnica presentada por el Unidad Administración Integral del Riesgo.*
> *Se instruye a la Administración a revisar los límites anualmente. De ser necesario deberán definirse límites por actividades de manera particular, según magnitud y frecuencia.*

Tolerancia al riesgo aceptable para procesos de Tecnologías de la Información

Mediante el acuerdo 3° de la sesión 984 realizada el miércoles 6 de mayo 2015 por la Junta Directiva, el cual indica lo siguiente:

> *Acuerdo 3°*
> *Con las recomendaciones de la Gerencia Genera, mediante el oficio GG-163-15, el acuerdo 5° del Comité de Riesgos en la sesión 402 y el oficio AR-38-15 del Área de Riesgos, se aprueba el informe Final de sobre la valorización de Riesgo Operativo para el área de TI de la OPC-CCSS para el segundo semestre de 2014*
>
> *Además, se aprueba el límite máximo tolerable de riesgo para el Área de Tecnologías de la información de un máximo de un 16.67%.*
>
> *Se le solicita a la Administración que se actualicen los documentos: 8PO04 Política de Riesgo Operativo y* ***8M04 Manual integral de procedimientos y políticas para la administración del riesgo para la OPC CCSS.***

La OPC-CCSS no deberá estar en niveles superiores a lo indicado en el cuadro que se presenta a continuación, y la periodicidad para la evaluación de riesgos operativos y riesgos tecnológicos realizada por el Área de Riesgos, será semestralmente y anualmente respectivamente.

Tolerancia Máxima Permitida	
Procesos OPC CCSS	Procesos de T.I.
3%	16.67%

Revisión de la Política de Riesgo Operativo

La Política de Riesgo Operativo deberá revisarse al menos una vez al año, con el fin de poder determinar la necesidad de ajustes. La Junta Directiva es la encargada de aprobar los ajustes sugeridos por el Área de Riesgos.

Mejoramiento Continuo

La OPC CCSS mejorará constantemente la eficacia de los procesos de riesgo operativo aplicando su Política de Calidad, los objetivos estratégicos, los resultados de la revisión por la dirección y las herramientas de análisis, medición y mejora, con el fin de contribuir al fortalecimiento continuo del Sistema de Gestión de Calidad.

DOCUMENTOS DE REFERENCIA

7PO06 Política General de Seguridad de la Información

CONTROL DE VERSIONES Y REVISIONES

Versión	Fecha de actualización	Fecha de revisión	Origen del cambio/ Resultado de la Revisión
07	12/09/16	N/A	Se agrega a la política el termino riesgo residual
08	27/07/17	N/A	Se elimina los eventos de riesgo operativo en tecnologías de la información, eventos de riesgos internos, eventos de riesgos con personas y eventos externos, en su lugar se incorporan los conceptos de evento e incidente operativo y eventos e incidente de seguridad de la información. Se agrega un cuadro de la tolerancia máxima permitida. Se incluye el apartado de documentos de referencia y se agrega el **8PO06 Política General de Seguridad de la Información**
09	04/07/18	N/A	Se actualiza la codificación de la política y los documentos de referencia de acuerdo con la nueva estructura de la ISO. Se incluye la clasificación documental en el pie de pagina Se incluye la columna de fecha de revisión en el control de versiones y revisiones

Aprobada por la Junta Directiva de la Operadora de Pensiones de la CCSS, en el acuerdo #5 de la sesión #1124, realizada el 27 de junio del 2018