8PO04
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 la Operadora, deberá de crear una reserva económica para la cobertura de los posibles eventos que se presenten.

1. Objetivo General

Administrar los riesgos operativos de manera que estos se mantengan dentro de los parámetros establecidos, según lo descrito en el documento **8F179 Declaratoria del Apetito al Riesgo**.

2. Objetivo Específicos

- Identificar, evaluar, medir, monitorear y controlar los eventos e incidentes 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 e incidentes 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.

3. Conceptos de riesgo operativo

De acuerdo con lo descrito en el documento **8E44 Reglamento de riesgos** en su artículo 3 definiciones, se define como riesgo operativo:

> *"…riesgo por fallas o deficiencias en los sistemas de información, controles internos, procesos internos, errores humanos, fraudes, fallos de gestión o alteraciones provocadas por acontecimientos externos. Incluye el riesgo de tecnologías de la información, el cual consiste en riesgos por daños, interrupción, alteración o fallas derivadas en los sistemas físicos e informáticos, aplicaciones de cómputo, redes y cualquier otro canal de distribución necesarios para la ejecución de procesos operativos por parte de las entidades reguladas"*

La Operadora de Pensiones Complementaria de la CCSS define los siguientes conceptos para clasificar los riesgos que afecten los objetivos pactados con el cliente, tanto interno como externo:

3.1 Incidente de Riesgo Operativo

Es la posibilidad de obtener pérdidas financieras relacionadas con el diseño inapropiado de los procesos, 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.

3.2 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.

Por otro lado, los conceptos de eventos e incidentes de seguridad de la información se encuentran establecidos dentro del documento **7P05 Procedimiento de Gestión de seguridad de la información** en el apartado 2.20 y se ejecutan de acuerdo con lo indicado en el documento **7PO06 Política General de seguridad de la información** en el apartado 2.21.

4. 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.

4.1 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.

4.2 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 efectividad del control al riesgo localizado. Los riesgos pueden ser

aceptados, mitigados o evitados de una manera consistente con la estrategia de la OPC-CCSS.

4.3 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.

4.4 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.

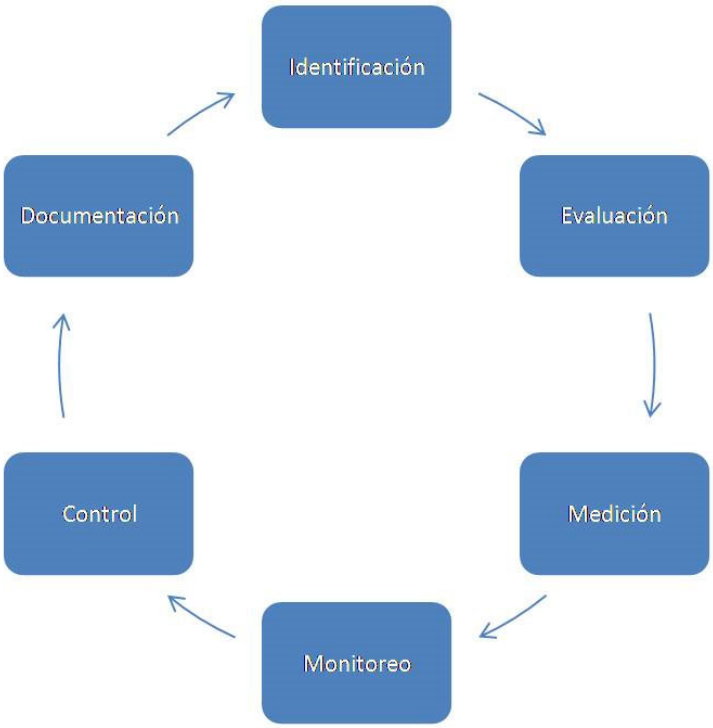
4.5 Control

Una vez identificados 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. Todas las deficiencias o desviaciones deben ser reportadas a la Gerencia.

4.6 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:



5. 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.

6. Estructura de Riesgos Operativos de la OPC CCSS

6.1 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.

6.2 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 el sistema de registro de casos de riesgos mediante el documento **8I30 Sistema de Control de riesgo Operativo,** en el cual se lleva el registro y seguimiento de las actividades significativas, generadoras de potenciales pérdidas que ocurren dentro de determinados eventos de riesgo, que podrían tener ocurrencia a lo largo de cada uno de los procesos, para estructurar mapas de riesgo institucionales.

6.3 Gestión del riesgo Legal

Para gestionar el riesgo legal, se realizará bajo el concepto descrito en el documento **8E44 Reglamento de Riesgos** en el artículo 3 el cual expone:

> *"**Riesgo legal**: Riesgo debido a la inobservancia o aplicación incorrecta o inoportuna de disposiciones legales o normativas, instrucciones emanadas de los organismos de control o como consecuencia de resoluciones judiciales, extrajudiciales o administrativas adversas, o de la falta de claridad o redacción deficiente en los textos contractuales que pueden afectar la formalización o ejecución de actos, contratos o transacciones"*

De acuerdo con lo mencionado, se deberá crear e implementar lineamientos y procedimientos para la medición y control de riesgo legal.

6.4 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.

6.5 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.

6.6 Apetito de Riesgo

La OPC CCSS no deberá estar en niveles superiores a lo indicado en el cuadro n°1 que se presenta a continuación, y la periodicidad para la evaluación de riesgos operativos y riesgos tecnológicos realizada por el Área de Riesgos, será semestral y anualmente respectivamente.

Cuadro n°1
Apetito al riesgo

Indicador	Apetito de Riesgo	Tolerancia	Capacidad
Riesgo Operativo en Procesos	<=1.34%	>1.34% y <2.40%	>= 2.40% y <3.96%
Riesgo Operativo en TI	<=12%	>12% y <15.50%	>= 15.50% y <16.67%

Fuente: 8F179 Declaratoria del Apetito al Riesgo

7. 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.

8. 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.

9. DOCUMENTOS DE REFERENCIA

8P05 Procedimiento de Gestión de seguridad de la información
8I30 Sistema de Control de riesgo Operativo,
8F179 Declaratoria del Apetito al Riesgo
7PO06 Política General de seguridad de la información
8E44 Reglamento de Riesgos

10. CONTROL DE VERSIONES Y REVISIONES

Versión	Fecha de actualización	Fecha de revisión	Origen del cambio/ Resultado de la Revisión
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
10	04/01/19	N/A	Se elimina los conceptos de evento e incidente de seguridad de la información ya que hacen estos se encuentran descritos en los documentos a 7I31 Instructivo de eventos e incidentes de seguridad de la información, 7P05 procedimiento de Gestión de la Seguridad de la información, Además se actualiza el documento en relación con el 8E44 Reglamento de Riesgo, específicamente en gestión de riesgo legal, concepto de riesgo operativo.
11	15/02/21	N/A	Se modifica el punto 6.6 apetito al riesgo, específicamente el cuadro N°1 y se alinea con referencia a 8F179 Declaratoria del Apetito al Riesgo y al 8M04, por otro lado, el punto 6.2 se modifica eliminando el concepto de la metodología AMA para incluir 8I30 Sistema de Riesgos Operativos.

Aprobada por la Junta Directiva de la Operadora de Pensiones de la CCSS, en el acuerdo #5de la sesión #1280 realizada el 2 de febrero del 2022