PROCESO: PLANEACIÓN ESTRATÉGICA
MANUAL DE GESTIÓN DEL RIESGO

OBJETIVO

Presentar la metodología y requisitos de aplicación para la administración de riesgos estratégicos, operacionales, transitorios y SARLAFT a los que se expone el FONCEP y que puedan afectar el cumplimiento de la Plataforma Estratégica.

ALCANCE

Los lineamientos descritos aplican para las dependencias, procesos y responsables de gestionar los riesgos estratégicos que incluyen riesgos de metas estratégicas y financieros; riesgos operacionales los cuales incluyen de gestión, corrupción, ambiental, Seguridad y Salud Ocupacional - SST y seguridad de la información; riesgos transitorios que incluyen los riesgos contractuales; y finalmente SARLAFT.

NORMATIVIDAD

- **Ley 80 de 1993: "**Por la cual se expide el Estatuto General de Contratación de la Administración Pública".
- **Ley 599 del 2000** "Por la cual se expide el Código Penal."
- **Documento Conpes 3714 de 2011** del Consejo Nacional de Política Económica y Social República de Colombia, Departamento Nacional de Planeación: "Del Riesgo Previsible En El Marco De La Política De Contratación Pública".
- **Decreto 1082 de 2015 "**Por medio del cual se expide el Decreto Único Reglamentario del Sector Administrativo de Planeación Nacional".
- **Decreto 1499 DE 2017** "Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015".
- **Norma Técnica Colombiana NTC-ISO 31000**, **2018**. Gestión del riesgo: directrices.
- **Decreto 807 de 2019** "Por medio del cual se reglamenta el Sistema de Gestión en el Distrito Capital y se dictan otras disposiciones".
- **Guía para la Administración del Riesgo Departamento Administrativo de la Función Pública (DAFP), octubre de 2020.** Guía para la administración del riesgo y el diseño de controles en Entidades públicas - Riesgos de gestión, corrupción y seguridad de la información - Versión 5.
- **Circular No.092 de 2020, Secretaria General de la Alcaldía Mayor de Bogotá** "Implementación del Sistema de Administración de Riesgos de Lavado de Activos y Financiación del Terrorismo -SARLAFT en las Entidades distritales".
- **Acuerdo 005 del 2020:** Por el cual se aprueba la Política de Gestión del Riesgo del Fondo de Prestaciones Económicas, Cesantías y
- Pensiones –FONCEP-"

- **Anexo 4 lineamientos para la gestión de riesgos de seguridad digital en entidades públicas -** Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital elaborado por el Departamento Administrativo de la Gestión Pública y Grupo Interno de Seguridad y Privacidad de la Información – Min TIC.
- **Decreto 830 de 2021** "Por el cual se modifican y adicionan los artículos al Decreto 1081 de 2015, Único Reglamentario del Sector Presidencia de la República, en lo relacionado con el régimen de las Personas Expuestas Públicamente (PEP)".

DEFINICIONES
Acciones de contingencia: Medidas que se establecen previamente para ejecutar una vez se materialice el riesgo, garantizando que se continúe la operación del proceso, metas, sistemas etc.
Acciones mejoramiento: Medidas que se establecen posterior al análisis de causas de un hallazgo o una autoevaluación, cuyo propósito es corregir los hechos materializados y prevenir que vuelvan a suceder.
Acciones de tratamiento: Medidas que buscan mitigar los riesgos mediante el fortalecimiento de los controles definidos.
Apetito de riesgo: Es el nivel de riesgo que la Entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la Entidad debe o desea gestionar. (DAFP, 2020)
Capacidad de riesgo: Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual la alta dirección considera que no sería posible el logro de los objetivos de la Entidad. (DAFP, 2020)
Causa: Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
Control: Medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones)
Financiación del Terrorismo (FT): Corresponde al conjunto de acciones que permiten la circulación de recursos que tienen como finalidad la realización de actividades terroristas o que pretenden el ocultamiento de activos provenientes de dichas actividades.
GAFI: Grupo de Acciones Financieras Internacionales
Impacto: Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo. Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la Entidad, sus grupos de valor y demás partes interesadas
Lavado de Activos (LA): Es el proceso mediante el cual organizaciones criminales buscan dar apariencia de legalidad a los recursos generados de sus actividades ilícitas.
Listas vinculantes o restrictivas: Es la relación de personas naturales y jurídicas que pueden estar vinculadas con actividades de lavado de activos o financiación del terrorismo.

Mapa de riesgos: Documento con la información resultante de la gestión del riesgo.
Operación inusual: Es aquella operación que se sale de los parámetros normales o que por su cuantía y características no guarda relación con la actividad económica o comercial de cada uno de los grupos de interés.
Personas Públicamente Expuestas (PEP): Personas nacionales o extranjeras que por su perfil o por las funciones que desempeñan pueden exponer en mayor grado a la Entidad al riesgo de LA/FT, tales como personas que por razón de su cargo manejan recursos públicos, detentan algún grado de poder público o gozan de reconocimiento público.
Probabilidad: Se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.
Reporte de Operaciones sospechosa (ROS): Corresponde a un hecho relacionado con la posible comisión de actividades relacionadas con los delitos de Lavado de Activos o Financiación del Terrorismo.
Riesgo: Efecto que se causa sobre los objetivos de las Entidades, debido a eventos potenciales. Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos. (DAFP, 2020)
Riesgo ambiental: Es aquel que se genera por la exposición a factores internos y externos que afectan el medio ambiente de la Entidad y organismo Distrital (contaminación, ambientes pocos saludables, malos hábitos) inherentes a las actividades propias de cada proceso.
Riesgo Contractual: El riesgo contractual en general es entendido como todas aquellas circunstancias que pueden presentarse durante el desarrollo o ejecución de un contrato y que pueden alterar el equilibrio financiero del mismo.
Riesgo de corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado o particular.
Riesgo de gestión: Posibilidad de que suceda algún evento que tenga impacto en el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencia (impacto).
Riesgos previsibles: Riesgos previsibles son todos los eventos que puedan afectar la realización de la ejecución contractual y cuya ocurrencia no puede ser redicha de manera exacta por parte de las partes involucradas en el proceso de contratación.
Riesgo de Seguridad de la información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000). (DAFP, 2020)
Riesgo inherente: Es aquel al que se enfrenta una Entidad en ausencia de acciones para modificar su probabilidad o impacto.
Riesgo residual: Nivel de riesgo que permanece luego de tomar los correspondientes controles o medidas de tratamiento (acciones en planes o relacionadas con indicadores).
Tolerancia del riesgo: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la Entidad.

UIAF: Unidad de Información y Análisis Financiero: es un organismo de inteligencia económica y financiera que centraliza, sistematiza y analiza la información suministrada por las Entidades que reportan y fuentes abiertas, para prevenir y detectar posibles operaciones de lavado de activos, sus delitos fuente, y la financiación del terrorismo.

CONTENIDO

DESARROLLO DEL MANUAL

I. CAPÍTULO 1. POLÍTICA DE GESTIÓN DEL RIESGO

La Política de Gestión del riesgo fue aprobada el 19 de agosto del 2020 por la Junta Directiva de FONCEP, cuya declaración es:

El Fondo de Prestaciones Económicas, Cesantías y Pensiones – FONCEP se compromete a gestionar integralmente sus riesgos mediante un enfoque preventivo y de control eficiente con el fin de garantizar el logro de los objetivos estratégicos, misionales e institucionales y la generación de valor público.

Alcance. La gestión integral de los riesgos se aplica considerando la cadena de valor institucional: resultados (objetivos estratégicos), productos (metas institucionales), procesos (modelo de operación por procesos incluyendo información crítica) e insumos donde el FONCEP realice y desarrolle actividades. Incluye riesgos de gestión, financieros, de corrupción, seguridad de la información, contractuales, ambientales, seguridad y salud en el trabajo y los que puedan generarse de acuerdo con la misionalidad.

Ciclo de la Gestión de riesgos. Para llevar a cabo la Gestión de los riesgos se han definido seis (6) etapas así:

I. **Identificación:** visibiliza los eventos que constituyen o pueden constituir una amenaza o variación negativa en el cumplimiento de los objetivos en los diferentes niveles establecidos.
II. **Análisis:** establece la probabilidad de ocurrencia (el número de veces que se ha presentado o puede presentarse en un periodo de tiempo determinado) y el impacto (gravedad de sus consecuencias o la magnitud de sus efectos), entre los cuales definen el riesgo inherente, es decir, suponiendo la ausencia de algún tipo de control.
III. **Evaluación (valoración):** establece el grado de exposición o nivel del riesgo y las opciones de manejo de cada uno, mediante la definición y valoración de los controles aplicados para la determinación del riesgo residual.
IV. **Tratamiento (manejo):** formulación de las acciones orientadas al mejoramiento de los controles o de implementación de nuevos controles, de acuerdo con el nivel residual y los niveles de aceptación definidos en esta política.
V. **Monitoreo y revisión:** revisión periódica de la eficacia de las acciones y los controles que se han implementado por las primeras líneas de defensa, identificando si se ha presentado la materialización de riesgos y su debido tratamiento.
VI. **Comunicación y consulta:** Etapa transversal a las anteriores orientada a la divulgación de la información pertinente al interior de la Entidad y a la participación de los grupos de valor relacionados.

Criterios para análisis de los riesgos. Los riesgos se identifican considerando los factores de probabilidad e impacto, cada uno de los cuales se analiza para cada riesgo considerando las siguientes escalas:

Tabla 1: Escala de probabilidad e impacto

Escala probabilidad	Escala impacto
Muy baja	Leve
Baja	Menor
Media	Moderado
Alta	Mayor
Muy Alta	Catastrófico

Fuente: Elaboración propia.

Nota: las variables y categorías de cada nivel tanto de probabilidad e impacto se encuentran en el desarrollo del presente documento.

Zonas de riesgo o niveles de exposición. Para determinar el nivel de exposición del riesgo, se usa la matriz de calor o mapa de riesgos, que combina los factores de probabilidad e impacto. FONCEP maneja 4 zonas de riesgos: extrema, alta, moderada y baja, las cuales se distribuyen como se ilustra en la tabla 2.

Tabla 2: Matriz de calor para la administración de riesgos en FONCEP

		Impacto				
Probabilidad		1	2	3	4	5
	5	Alta	Alta	Alta	Alta	Extrema
	4	Moderada	Moderada	Alta	Alta	Extrema
	3	Moderada	Moderada	Moderada	Alta	Extrema
	2	Baja	Moderada	Moderada	Alta	Extrema
	1	Baja	Baja	Moderada	Alta	Extrema

Fuente: Elaboración propia a partir de la información del Guía para la administración del riesgo y el diseño de controles en Entidades públicas del DAFP (2020).

Determinación de la capacidad de riesgo
Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la alta dirección que no sería posible el logro de los objetivos de la Entidad. Para el FONCEP, se establece los siguientes niveles.

- Apetitivo: riesgos cuyo nivel residual es bajo.
- Tolerancia: riesgos cuyo nivel residual es moderado.
- Capacidad: son todos los niveles de riesgos incluyendo el residual es alta y extrema.

Lo anterior, está dado por la definición de criterios de impacto, los cuales se adecuaron a la realidad dl FONCEP desde un estudio técnico de impacto por cada una de las áreas que se ve representado en la tabla 8.

Nivel de aceptación al riesgo (apetito del riesgo)[1] Los riesgos en niveles de exposición "moderado", "alto" o "extremo" son inaceptables y deben ser tratados de acuerdo con una de las opciones de manejo establecidas (evitar, reducir o compartir el riesgo). Los riesgos de corrupción son inaceptables, independientemente de su nivel y deben ser tratados.

Tratamiento (manejo) de riesgos. De acuerdo con el nivel de exposición en que se encuentre cada riesgo y la relación costo-beneficio de las medidas de tratamiento, se define la opción de manejo a realizar. Solo puede tratarse el riesgo con un solo tipo de opción de tratamiento, estas son:

- Aceptar el riesgo: no se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (Ningún riesgo de corrupción podrá ser aceptado).
- Evitar el riesgo: se abandonan las actividades que dan lugar al riesgo, es decir, no se inicia o no se continúa con la actividad que lo provoca.
- Reducir el riesgo: se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles.
- Compartir o transferir el riesgo: se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad.

En este sentido, ante un riesgo que derive en un riesgo residual que supere el nivel aceptable se deberá volver a analizar y revisar dicho tratamiento. En todo caso para los riesgos superiores a categorización "baja", se deberá evitar compartir o reducir el riesgo.

[1] Apetito de riesgo: es el nivel de riesgo que la Entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la Entidad debe o desea gestionar.

Periodicidad del seguimiento. El seguimiento a los riesgos asociados a posibles actos de corrupción debe darse dando cumplimiento a la periodicidad establecida por la normatividad colombiana, y los lineamientos de la secretaria de Transparencia de la Presidencia de la República y el Departamento Administrativo de la Función Pública. Para los demás tipos de riesgos el monitoreo y seguimiento se realizarán a través de las líneas de defensa y según lo establecido en el presente manual y documentación asociada a la gestión del riesgo de FONCEP.

Responsabilidades. La responsabilidad está definida mediante las líneas de defensa y en la Entidad se acogen a la siguiente tabla:

Tabla 3: Líneas de defensa, responsables y responsabilidades

Líneas De Defensa	Responsables	Responsabilidad Frente Al Riesgo
Línea estratégica	• Junta Directiva. • Alta Dirección. • Comité Asesor de la Dirección y Experiencia a la Ciudadanía. • Comité Institucional de Gestión y Desempeño • Comité Institucional de Coordinación de Control Interno (CICCI).	- Gobernar la gestión del riesgo - Definir el marco general para la gestión del riesgo y el control a través del establecimiento de la Política de Gestión del Riesgo. - Asegurar y supervisar el cumplimiento de la política en todos los niveles de la organización. - La alta dirección y el Comité Institucional de Coordinación de Control Interno - CICCI, de manera articulada deben definir lineamientos en las siguientes materias: gestión del riesgo (o política institucional de riesgos); comunicaciones (internas y externas;, estatuto de auditoría; anticorrupción (fraude y corrupción); talento humano; planeación estratégica; productos y servicios de la entidad; generación de alertas y recomendaciones al Comité Institucional de Gestión y Desempeño para la mejora de la gestión; y la programación, ejecución y seguimiento presupuestal. - El CICCI debe establecer lineamientos para el funcionamiento del Sistema de Control Interno-SCI, aprobar el Plan Anual de Auditoría, la metodología para documentar y formalizar el esquema de línea de defensa, generar alertas al CIGD a partir de los resultados y evaluación del SCI, monitorear el cumplimiento de los estándares de conducta y práctica de los principios y valores

Líneas De Defensa	Responsables	Responsabilidad Frente Al Riesgo
		del servicio público, revisar la exposición de la entidad a los riesgos de corrupción y fraude, verificar el cumplimiento de los lineamientos de gestión del riesgo. - El CICCI debe: fomentar la divulgación e implementación de la política de administración del riesgo; monitorear el cumplimiento de la política de administración de riesgos de la entidad; promover la identificación y análisis del riesgo desde el direccionamiento o planeación estratégica; monitorear los cambios en el entorno (interno y externo) que puedan afectar la efectividad del SCI; monitorear el estado de los riesgos aceptados (apetito por el riesgo) con el fin de identificar cambios sustantivos que afecten el funcionamiento de la entidad; monitorear el seguimiento a la gestión del riesgo por parte de las instancias responsables; fomentar la promoción de los espacios para capacitar a los líderes de los procesos y sus equipos de trabajo sobre la metodología de gestión del riesgo; fomentar la generación de acciones para apoyar a la segunda línea de defensa frente al seguimiento del riesgo -
Primera línea	• Líderes de proceso • Gerentes de meta • Referente ambiental • Referente de Seguridad y Salud en el Trabajo • Supervisores de contrato • Comité Fiduciario de Seguimiento de Pensiones y Cesantías.	- Implementar procesos de gestión y control de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora. - Diseñar, implementar y monitorear la ejecución de controles. - Gestionar de manera directa en el día a día los riesgos de la Entidad. - Reportar a la segunda línea de defensa los avances y dificultades de la gestión del riesgo, además de los riesgos materializados. - Divulgar y sensibilizar al interior de sus dependencias el mapa de riesgos junto con el plan de manejo. - Cumplir lineamientos para generar y comunicar información que facilite las acciones de control; comunicar información relevante

Líneas De Defensa	Responsables	Responsabilidad Frente Al Riesgo
		de manera oportuna, confiable y segura; utilizar los mecanismos de comunicación definidos por la entidad para interactuar con los grupos de valor y entes de control. - Hacer seguimiento a los riesgos y controles para identificar deficiencias y proponer ajustes; e informar el desempeño de las actividades de gestión de riesgos.
Segunda línea	• Jefe Oficina Asesora de Planeación • Jefe Oficina Asesora Jurídica • Jefe Oficina de Informática y Sistemas • Subdirector Financiero y Administrativo • Servidores que tengan responsabilidades directas en el monitoreo y evaluación de los controles. • Cargos que lideran temas estratégicos de gestión como jefes de planeación, financieros, contratación, tecnología e información, servicios al ciudadano u otros sistemas de gestión.	- Asesorar a la línea estratégica en el análisis del contexto de la Entidad, definición del marco general de la gestión del riesgo. - Definir el esquema operativo para la gestión del riesgo, para facilitar el cumplimiento de la Política. - Acompañar y supervisar permanentemente a la primera línea de defensa en el ciclo de la gestión del riesgo. - Asegurar que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados y se ejecuten apropiadamente. - Monitorear la gestión de riesgo y controles ejecutada por la primera línea de defensa. - Socializar los resultados de la gestión del riesgo (mapa e informes) a los grupos de valor. - Impulsar la cultura de gestión del riesgo. - Verificar la adecuada identificación y valoración de riesgos frente al logro de objetivos, metas institucionales; aquellos relacionados con fraude y corrupción, - Generar recomendaciones a las instancias correspondientes, así como monitorear y evaluar las exposiciones a los riesgos relacionados con tecnología nueva y emergente. - Verificar el diseño de controles que sean pertinentes frente a los riesgos; verificar que los controles contribuyan a la mitigación de todos los riesgos; asegurar que los riesgos sean monitoreados según la política de riesgos; hacer seguimiento a los mapas de riesgo y verifica que se encuentre actualizado,

Líneas De Defensa	Responsables	Responsabilidad Frente Al Riesgo
		- Proponer acciones de mejora para mejorar el diseño o ejecución de los controles; verificar que los responsables estén ejecutando los controles tal como han sido diseñados; verificar el diseño y ejecución de los controles que mitigan los riesgos estratégicos o institucionales; verificar el diseño y ejecución de los controles que mitigan los riesgos de fraude y corrupción. - Comunicar a la alta dirección y a los distintos niveles de la entidad, los eventos en materia de información y comunicación que afectan el funcionamiento del control interno; verificar que la información fluye, a través de los canales establecidos, de manera accesible, oportuna, confiable, íntegra y segura dentro de la entidad, que respalde el funcionamiento del sistema de control interno; apoyar el monitoreo de canales de comunicación, incluyendo líneas telefónicas de denuncias. - Verificar que las acciones de mejora respondan a las observaciones de los entes de control; verificar que las acciones de mejora se realicen por parte de los responsables, y que sean efectivas y contribuyan al logro de los resultados.
Tercera línea	Jefe Oficina de Control Interno	- Proporcionar información sobre la efectividad del Sistema de Control Interno a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa. - Proporcionar un aseguramiento basado en el más alto nivel de independencia y objetividad sobre la efectividad del Sistema de Control Interno. - Asesorar a la primera línea de defensa en coordinación con la segunda línea de defensa en la implementación del ciclo de gestión del riesgo. - Adelantar seguimiento a los riesgos de la institución verificando la efectividad de los controles. - Recomendar mejoras a la política de operación para la administración del riesgo.

Fuente: Elaboración propia a partir de la información de la Guía para la administración del riesgo y el diseño de controles en Entidades públicas del DAFP (2020)

Comunicación y consulta

Las actividades de comunicación y consulta con los grupos de valor tienen lugar durante todas las etapas de la gestión del riesgo. Estas actividades están dadas por los reportes periódicos y su divulgación de acuerdo con la normatividad existente y las necesidades de FONCEP. Dentro de estas actividades están:

- Divulgación del mapa de riesgos para consulta al interior de la Entidad.
- Socialización de los riesgos con el equipo de trabajo por parte de los líderes y responsables de cada proceso.
- Socialización de las metodologías de identificación y gestión del riesgo, y fortalecimiento de la cultura del riesgo por parte de la Oficina Asesora de Planeación y la Oficina de Control Interno.
- Consulta y divulgación del mapa de riesgos de corrupción a los grupos de valor a través de su publicación en la página web en el enlace de transparencia.
- Las demás actividades establecidas en la documentación asociada a la gestión del riesgo (manual, instructivos, guías, procedimientos, entre otros.)

Operación de la Política de Gestión de Riesgos. La operación de esta política está descrita en el presente manual y demás documentos asociados a la Gestión Integral de Riesgos de FONCEP.

II. CAPÍTULO 2. GENERALIDADES

Tipología de riesgos. El presente documento es la herramienta para la gestión integral de los riesgos en el Fondo de Prestaciones Económicas, Cesantías y Pensiones – FONCEP.

Frente a lo anterior, es necesario señalar que en un sentido amplio el riesgo es definido como: “efecto que se causa sobre los objetivos de las Entidades, debido a eventos potenciales”. FONCEP podría verse afectado por riesgos en los objetivos estratégicos o metas institucionales, la misionalidad de la Entidad por hechos de corrupción, el modelo financiero por la naturaleza de la Entidad, los objetivos de cada uno de los procesos, los objetivos de los sistemas de gestión tales como seguridad de la información, ambiental o seguridad y salud en el trabajo y, finalmente, el equilibrio económico contractual.

Por lo anterior, teniendo en cuenta la cadena de valor de la Entidad y en concordancia con la política establecida, el FONCEP reconoce riesgos estratégicos, operacionales y transitorios, como se muestra en la siguiente tabla:

Tabla 4: Riesgos FONCEP

Cadena De Valor	Nivel	Clase	Nivel De Gestión
Resultados y Productos	Estratégicos	Metas y resultados	Resultados, productos, líneas de acción, Metas Institucionales
		Fiduciarios y financieros	Modelo Financiero
Actividades	Operacionales	Procesos (objetivos y salidas)	Todos los Procesos
		Corrupción	Procesos susceptibles a hechos de corrupción
		Ambiental	Procesos con responsabilidad ambiental
		Seguridad de la información	Procesos responsables de grupos de activos de Información
		Seguridad y salud en el trabajo (SST)	Procesos con responsabilidad de gestión en SST
Insumos	Transitorios	Contractuales	Inherentes a la ejecución de Contratos
	SARLAFT	SARLAFT	Inherente a la adquisición de bienes y servicios

Fuente: Elaboración propia

Roles y Responsabilidades. Una vez descritos los tipos de riesgos, es pertinente enunciar las responsabilidades y roles según la tipología de riesgos. Para ello es necesario explicar el modelo de "líneas de defensa" adoptado por el Departamento Administrativo de la Función Pública-DAFP, en el cual fundamenta una estrategia para garantizar el cumplimiento de la gestión riesgos mediante la definición de roles y responsabilidades de los actores que intervienen en la gestión, su supervisión y el aseguramiento independiente. La tabla siguiente muestra la estructura del modelo de líneas de defensa.

Tabla 5: Niveles, roles y responsabilidades según riesgos

Niveles De Riesgos		Roles y Responsabilidades		
Nivel	**Clase**	**Primera Línea**	**Segunda Línea**	**Tercera Línea**
Estratégicos	Metas y resultados	Responsables Objetivos o Gerentes de Meta	Jefe Oficina Asesora de Planeación	Jefe Oficina de Control Interno
	Fiduciarios y financieros	Comité Fiduciario de Seguimiento de Pensiones y Cesantías	Subdirector Financiero y Administrativo	
Operacional	Corrupción	Líderes Proceso	Jefe Oficina Asesora de Planeación	
	Procesos (objetivos y salidas)	Líderes Proceso	Jefe Oficina Asesora de Planeación	
	Ambiental	Referente Ambiental Asesor responsable Gestión Administrativa	Subdirector Financiero y Administrativo	
	Seguridad de la información	Responsable grupo de activos	Jefe Oficina de Informática y Sistemas	
	Seguridad y salud en el trabajo-SST	Líder SST Asesor responsable de Talento Humano	Subdirector Financiero y Administrativo	
Transitorios	Contractuales	Supervisores de Contrato	Jefe Subdirección Jurídica	
SARLAFT	SARLAFT	Supervisores de Contrato	Jefe Subdirección Jurídica	

Fuente: Elaboración propia

Nota: Dentro de la política de gestión del riesgo se encuentran las responsabilidades generales por cada una de las líneas de defensa.

A continuación, se presentan funciones, roles, responsabilidades y autoridad por la línea de defensa aplicando el modelo del DAFP.

Línea de defensa estratégica.

- **Función**: Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento.
- **Rol**: Alta Dirección (Comités Directivos, Comité Institucional de Gestión y Desempeño, el Comité Institucional de Coordinación de Control Interno).
- **Responsabilidad**: Analizar los riesgos y amenazas institucionales para el cumplimiento de los planes estratégicos. Definir el marco general para la gestión del riesgo (política de administración del riesgo) y garantizar el cumplimiento de los planes de la Entidad.

Primera Línea de Defensa.

- **Función**: Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, evaluación, monitoreo y acciones de mejora.
- **Rol**: Líderes de los procesos, programas y proyectos de la Entidad, gerentes de meta, supervisores de contratos, líder SST, Comité Fiduciario, referente ambiental.
- **Responsabilidad**: Diseñar, implementar y monitorear los controles; gestionar de manera directa en el día a día los riesgos de la Entidad través de su identificación, análisis, evaluación, monitoreo y acciones de mejora. Orientar el desarrollo e implementación de políticas y procedimientos internos y asegurar que sean compatibles con las metas y objetivos de la Entidad y emprender las acciones de mejoramiento para su logro.
- **Autoridad**: Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora.

Segunda Línea de Defensa.

- **Función**: Asegura que los controles y los procesos de gestión de riesgo implementados por la primera línea de defensa estén diseñados apropiadamente y funcionen como se pretende.
- **Rol**: Servidores que tienen responsabilidades directas en el monitoreo, evaluación de los controles y la gestión del riesgo, jefe de Oficina Asesora de Planeación, jefe de Oficina Asesora Jurídica (contractual), jefe Oficina de Informática y Sistemas (Seguridad de la información), coordinadores de otros sistemas de gestión de la Entidad (Seguridad y Salud en el Trabajo y Sistema de Gestión Ambiental). Los jefes que cuenten con rol de segunda línea de defensa podrán asignar a profesionales que apoyen su función y responsabilidad.

- **Responsabilidad**: Monitorear la gestión del riesgo y control ejecutado por la primera línea de defensa, complementando su trabajo.
- **Autoridad**: Asegurar que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa estén diseñados apropiadamente y funcionen como se pretende; asistir y guiar la primera línea de defensa en la gestión adecuada de los riesgos que pueden afectar el cumplimiento de los objetivos institucionales y de sus procesos, incluyendo los riesgos de corrupción, a través del establecimiento de directrices, apoyo en el proceso de identificar, analizar, evaluar y tratar los riesgos y realiza un monitoreo independiente al cumplimiento de las etapas de la gestión de riesgos; reporta el estado de los riesgos a la línea estratégica para la toma de decisiones.

Tercera Línea de Defensa.

- **Función:** Proporciona información sobre la efectividad del Sistema de Control Interno-SCI a través de un enfoque basado en riesgo incluida la operación de la primera y segunda línea de defensa.
- **Rol**: Oficina de Control Interno.
- **Responsabilidad**: Proporcionar aseguramiento basado en el más alto nivel de independencia y objetividad sobre la efectividad del SCI; adelantar seguimiento al Mapa de Riesgos de Corrupción, a la gestión del riesgo, verificando la efectividad de los controles, antes de los primeros 10 días de cada cuatrimestre.
- **Autoridad**: Proporcionar información sobre la efectividad del SCI, a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa; provee aseguramiento (evaluación) independiente y objetiva sobre la efectividad de la gestión de riesgos, validando que la línea estratégica, la primera y segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos para el logro en el cumplimiento de los objetivos institucionales y de proceso.

III. CAPÍTULO 3. ETAPAS DE LA ADMINISTRACIÓN DEL RIESGO (CICLO DE LA GESTIÓN DEL RIESGO)

La gestión del riesgo al interior de FONCEP, identifica los riesgos que pueden afectar el cumplimiento de los objetivos estratégicos y de proceso, identifica causas o fallas que pueden dar origen a la materialización del riesgo, identifica el riesgo inicial o inherente. El paso siguiente consiste en identificar el control o controles y finalmente, evaluar si los controles están bien diseñados para mitigar el riesgo y si estos se ejecutan como fueron diseñados determinando simultáneamente el riesgo residual. En otras palabras, la gestión del riesgo se hace de acuerdo con el siguiente esquema de etapas siguiéndolo en sentido de las manecillas del reloj.

Ilustración 1: **Ciclo de gestión de riesgos**

Fuente: Elaboración propia

1. **Identificación.** Visibiliza los eventos que constituyen o pueden constituir una amenaza o variación negativa en el cumplimiento de los objetivos en los diferentes niveles establecidos. En esta etapa se deben establecer las fuentes o factores de riesgo, los eventos o riesgos, sus causas y sus consecuencias. Para el análisis se deben tener en cuenta datos históricos, análisis teóricos, opiniones informadas, expertas y necesidades de las partes involucradas. Esta etapa está dividida en dos partes, el establecimiento del contexto y la identificación del riesgo.

Para el *establecimiento del contexto* se deben definir los parámetros internos y externos que se han de tomar en consideración para la administración del riesgo, pues a partir de estos se establecen las posibles causas o riesgos a identificar. El producto principal de esta etapa es el Plan Estratégico Institucional y los ejercicios de planeación estratégica, además, el seguimiento a estos en los espacios de la Alta Dirección definidos por FONCEP; por ejemplo, el Comité de Gestión y Desempeño, Comité Asesor de la Dirección y Experiencia a la Ciudadanía, y los demás comités de la alta dirección. Sin embargo, este no es el único insumo para establecer el contexto, también cada proceso según su particularidad en sus Comités Primarios y demás reuniones podrían identificar elementos internos y externos que generen claridad de las características del proceso y cumplimiento de este requisito.

Para la *identificación del riesgo* se describe el nombre del riesgo, las causas y efectos e impacto de cada uno de ellos. Para ello es necesario tener en cuenta la tipología de riesgos teniendo en cuenta lo mencionado en los capítulos correspondientes de este documento.

NOTA: Los riesgos deben estar descritos de manera clara y precisa, su redacción no debe dar lugar a ambigüedades o confusiones.

2. **Análisis.** En esta etapa se busca establecer la probabilidad de ocurrencia del riesgo (el número de veces que se ha presentado o puede presentarse en un periodo de tiempo determinado) y sus consecuencias o impacto (gravedad de sus consecuencias o la magnitud de sus efectos) con el fin de estimar la zona de riesgo inicial (riesgo inherente), es decir, se realiza suponiendo la ausencia de algún tipo de control.

Análisis de la probabilidad. se entiende como la posibilidad de ocurrencia del riesgo. Para efectos de este análisis, la probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año. Para lo anterior, se debe tener en cuenta la siguiente tabla:

Tabla 6: Criterios para calificar probabilidad

Nivel	Escala	Descripción	Cualitativa
1	Muy baja	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año	20%
2	Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
3	Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
4	Alta	La actividad que con lleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
5	Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Fuente: Tomado de la Guía para la administración del riesgo y el diseño de controles en Entidades públicas del DAFP (2020).

A continuación, se muestra una tabla de actividades típicas relacionadas con la gestión de una Entidad pública, bajo las cuales se definen las escalas de probabilidad, como ejemplo de la aplicación

Tabla 7: Actividades típicas en la gestión pública

Actividad	Frecuencia de la Actividad	Probabilidad frente al Riesgo
Planeación estratégica	1 vez al año	Muy baja
Actividades de talento humano, jurídica, administrativa	Mensual	Media
Contabilidad, cartera	Semanal	Alta
Tecnología (incluye disponibilidad de aplicativos), tesorería	Diaria	Muy alta

Fuente: Tomado de la Guía para la administración del riesgo y el diseño de controles en Entidades públicas del DAFP (2020).

Análisis de consecuencias o nivel de impacto. Por impacto se entienden las consecuencias que puede ocasionar a la organización la materialización del riesgo.

En este caso

- Se tienen en cuenta las consecuencias potenciales establecidas en la identificación del riesgo.
- Para su determinación se utiliza la tabla de niveles de impacto establecida la tabla 8.

Cuando se presente más de un impacto para un riesgo con diferentes niveles se debe tomar el nivel más alto. Para analizar el impacto se deben tener en cuenta las siguientes tablas de niveles de impacto que también se encuentran en la Política de Riesgos. Adicional a esto, cuando se identifiquen varios criterios de impacto en el mismo nivel y este sea el más alto, se debe escoger teniendo en cuenta lo siguiente:

1. El impacto más directo o relacionado con el riesgo
2. Si con lo anterior no se identifica, se debe escoger aquel que se encuentre asociado al criterio de imagen o de afectación de presupuesto

Tabla 8: Criterios para calificar el impacto

Escala	Estratégico y de proceso	Tecnológico (indisponibilidad)	Tecnológico (triada)	Imagen	Atención a PQRSD, trámites y servicios	Tiempo promedio de atención	Legal	Contractual	Jurídico	Talento Humano	Afectación presupuesto inversión	Afectación presupuesto funcionamiento	Impacto Misional	Elementos de control
Leve 20%	Cambios de actividades planeadas inicialmente (fechas, entregables o eliminación)	Se presenta indisponibilidad de servicios de hasta ocho (8) horas, que afecte el interior de FONCEP	•Pérdida de información que se recupera en su totalidad •Asignación errada de controles de acceso por parte de FONCEP en información pública •Modificaciones y/o alteraciones en los activos, cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la Entidad o entes externos	Imagen institucional interna afectada por un área de la Entidad	Incumplimiento de los términos y criterios de respuesta en tres solicitudes del total de recibidas en el mes	Afectación de la atención a un ciudadano en un tiempo superior a 20 minutos promedio	Genera multas a las partes	Incumplimiento parcial, defectuoso o tardío de las obligaciones del contrato que no afecta el cumplimiento del objeto contractual	Pago de sanciones, indemnizaciones o demandas que afectan el presupuesto de la Entidad en un valor ≥10%	Se genera afectación en salud y ausentismos debido a enfermedades o accidentes laborales entre 0 y 10 días de incapacidad	Si representa hasta 10% del presupuesto de inversión asignado en la vigencia	Si representa hasta 2% presupuesto de funcionamiento asignado en la vigencia	*Inoportunidad de atención de **solicitudes interna**s, que no comprometan decisiones en el reconocimiento y pago prestacional	Identificación de desviaciones, inconsistencias, incumplimientos de las actividades del proceso
Menor 40%	Incumplimiento de las fechas estimadas de inicio del Plan Anual de Adquisiciones	Se presenta indisponibilidad de servicios hasta de cuarenta y ocho (48) horas, que afecte el interior de FONCEP	•Pérdida de información que se recupera parcialmente •Asignación de controles de acceso erróneos por parte de FONCEP en información clasificada y/o pública, pero no fue accedida por personas no autorizadas, y por lo tanto no fue divulgada •Modificaciones y/o alteraciones en los activos, cuya pérdida de exactitud y completitud conlleva un impacto significativo, ya que la información fue publicada y comunicada de forma errónea	Imagen institucional afectada internamente	Incumplimiento de los términos y criterios de respuesta en cinco solicitudes del total de recibidas en el mes	Afectación de la atención a un ciudadano en un tiempo hasta 30 minutos promedio	Posibles demandas para las partes	Ejecución parcial o baja del contrato que pueden ser subsanadas mediante medidas legales o que conlleve a la suspensión del contrato	Pago de sanciones, indemnizaciones o demandas que afectan el presupuesto de la Entidad en un valor ≥15%	Se genera afectación en salud y ausentismos debido a enfermedades o accidentes laborales catalogados según su gravedad y/o severidad como leves. Lo que quiere decir que puede generar de 11 a 30 días de incapacidad	Si representa hasta 15% del presupuesto de inversión asignado en la vigencia	Si representa hasta el 4% del presupuesto de funcionamiento asignado en la vigencia	***Inoportunidad** en la atención de **solicitudes interna**s, que puedan comprometer, con baja incidencia, las decisiones finales en el reconocimiento y pago prestacional **Falta de **claridad** en los conceptos que sirven de insumo posterior para el reconocimiento y pago prestacional *** **Recomendaciones realizadas** por la OCI en informes de control interno, para el mejoramiento del proceso de reconocimiento y pago prestacional ****I**ncremento del número de PQRSD** formulados por los ciudadanos, por falta de claridad en decisiones previamente adoptadas en el proceso de reconocimiento y pago prestacional	Investigaciones disciplinarias derivadas de desviaciones, inconsistencias, incumplimientos de las actividades del proceso
Moderado 60%	Incumplimiento de salidas de procesos o Incumplimiento del Plan de Acción Institucional	Se presenta indisponibilidad de servicios hasta noventa y seis (96) horas, que afecte la prestación del servicio de FONCEP	•Pérdida de información clasificada, que se recupera totalmente •Asignación de controles de acceso erróneos por parte de FONCEP en información clasificada y/o pública, pero fue divulgada al interior de la Entidad •Modificaciones y/o alteraciones en los activos, cuya pérdida de exactitud y completitud conlleva a acciones de índole legal o económico, retrasar sus funciones, o generar pérdidas de imagen moderado de la Entidad.	Imagen institucional afectada entre los grupos de valor de FONCEP	Incumplimiento de los términos y criterios de respuesta en ocho solicitudes del total de recibidas en el mes	Afectación de la atención a un ciudadano en un tiempo hasta 35 minutos promedio	Inicio de investigación disciplinaria a servidores del FONCEP	Demoras en la ejecución del contrato, pero no afecta el beneficio para las partes	Pago de sanciones, indemnizaciones o demandas que afectan el presupuesto de la Entidad en un valor ≥20%	Se genera afectación en salud y ausentismos debido a enfermedades o accidentes laborales catalogados según su gravedad y/o severidad como severo. Lo que quiere decir que puede generar de 31 a 90 días de incapacidad	Si representa hasta 20% del presupuesto de inversión asignado en la vigencia	Si representa hasta el 7% del presupuesto de funcionamiento asignado en la vigencia	** **Incremento del número de PQRSD** formulados por los ciudadanos, por falta de claridad en decisiones previamente adoptadas en el proceso de reconocimiento y pago prestacional ***Hallazgos administrativo**s, en firmes, decretados por la OCI u organismos de control, por causa y/o con ocasión del proceso de reconocimiento y pago prestacional.	Sanciones disciplinarias, fiscales y/o penales que impidan el cumplimiento del plan de acción institucional
Mayor 80%	Incumplimiento de indicadores de metas estratégicas	Se presenta indisponibilidad de servicios de hasta ciento veinte (120) horas, que afecte la prestación del servicio de FONCEP	•Pérdida de información clasificada o reservada, que se recupera parcialmente •Información catalogada como clasificada o reservada accedida por alguien no autorizado de carácter externo •Modificaciones y/o alteraciones en los activos, cuya pérdida de exactitud y completitud conlleva un impacto significativo, ya que la información fue publicada y comunicada de forma errónea, y se generó una investigación por entes de control	Imagen institucional afectada a nivel distrital	Incumplimiento de los términos y criterios de respuesta en diez solicitudes del total de recibidas en el mes	Afectación de la atención a un ciudadano en un tiempo hasta 40 minutos promedio	Procesos de investigación fiscal a servidores del FONCEP y contratistas	Retrasa la ejecución del contrato afectando de manera directa el beneficio de las partes	Pago de sanciones, indemnizaciones o demandas que afectan el presupuesto de la Entidad en un valor ≥30%	Se genera afectación en salud y ausentismos debido a enfermedades o accidentes laborales catalogados según su gravedad y/o severidad como grave. Lo que quiere decir que puede generar de 91 o más días de incapacidad	Si representa hasta 25% del presupuesto de inversión asignado en la vigencia	Si representa hasta el 15 % del presupuesto de funcionamiento asignado en la vigencia	*Inoportunidad en la atención de solicitudes de reconocimiento prestacional, no mayor a la mitad del plazo inicialmente establecido en la ley para emitir decisión, y sin que se decrete ampliación justificada del término, conforme a la ley **Inoportunidad en la atención de solicitudes de pago prestacional, no mayor a la mitad del plazo inicialmente establecido en la ley para realizar el pago, y sin que se decrete ampliación justificada del término, conforme a la ley ***Apertura de procesos administrativos sancionatorios, fiscales, disciplinarios o penales**, por el incorrecto e inoportuno reconocimiento y pago prestacional ****Hallazgos disciplinarios, fiscales y penales**, en firmes, decretados por la OCI u organismos de control, por causa y con ocasión del proceso de reconocimiento y pago prestacional	Sanciones disciplinarias, fiscales y/o penales que impidan el cumplimiento de las metas distritales y generen afectación reputacional
Catastrófico 100%	Incumplimiento de lo establecido (resultados) en el Plan de Desarrollo Distrital	Se presenta indisponibilidad de servicios de más de ciento veinte (120) horas, que afecte la prestación del servicio de FONCEP	•Pérdida de información que no se recupera •Información catalogada como clasificada o reservada accedida por alguien no autorizado, fue publicada y usada generando una afectación grave en la reputación en FONCEP •Modificaciones y/o alteraciones en los activos, cuya pérdida de exactitud y completitud conlleva a inconvenientes de índole legal o económico, retrasar las funciones o generar pérdidas de imagen severas de la Entidad	Imagen institucional afectada a nivel nacional	Incumplimiento de los términos y criterios de respuesta en quince solicitudes del total de recibidas en el mes	Afectación de la atención a un ciudadano en un tiempo superior a 50 minutos promedio	Intervención - sanción a los servidores de FONCEP y los contratistas	Paraliza la ejecución del contrato y afecta de manera directa el cumplimiento del objeto contractual	Pago de sanciones, indemnizaciones o demandas que afectan el presupuesto de la Entidad en un valor ≥40%	Se genera afectación en salud, produciendo consecuencias mortales por enfermedades o accidentes laborales. Lo que quiere decir que genera la muerte	Si representa más del 25% o más del presupuesto de inversión asignado en la vigencia	Si representa más del 15% del presupuesto de funcionamiento asignado en la vigencia	*Inoportunidad en la atención de solicitudes de reconocimiento prestacional, que supere el doble del plazo inicialmente establecido en la ley para emitir decisión, y sin que se decrete ampliación justificada del término, conforme a la ley, o no medie justificación racional del vencimiento en esas condiciones **Inoportunidad en la atención de solicitudes de pago prestacional, que supere el doble del plazo inicialmente establecido en la ley para realizar el pago, y sin que se decrete ampliación justificada del término, conforme a la ley, o no medie justificación racional del vencimiento en esas condiciones ***Sanciones disciplinarias, fiscales o penales**, en firmes, ocasionadas por el incorrecto e inoportuno reconocimiento y pago prestacional	

Fuente: Elaboración propia a partir de la información de la Guía para la administración del riesgo y el diseño de controles en Entidades públicas del DAFP (2020).

Sede Principal
Carrera 6 Nro. 14-98
Edificio Condominio Parque Santander
Teléfono: +571 307 62 00 || **www.foncep.gov.co**

ALCALDÍA MAYOR DE BOGOTÁ D.C.
FONDO DE PRESTACIONES ECONÓMICAS, CESANTÍAS Y PENSIONES

3. **Evaluación (valoración).** Establece el grado de exposición o nivel del riesgo y las opciones de manejo de cada uno, mediante la definición y valoración de los controles aplicados para la determinación del riesgo residual. Lo anterior, mediante la definición del **riesgo antes y después de controles**.

Riesgo antes de controles. Se identifica la zona de riesgo inicial (inherente) o la zona de riesgo sin controles, mediante el cruce de las variables de probabilidad e impacto explicado en la etapa anterior de análisis. Dicho cruce se realiza sobre la matriz de calor que se muestra a continuación.

Tabla 9: Matriz de calor de riesgos

		Impacto				
Probabilidad		1	2	3	4	5
	5	Alta	Alta	Alta	Alta	Extrema
	4	Moderada	Moderada	Alta	Alta	Extrema
	3	Moderada	Moderada	Moderada	Alta	Extrema
	2	Baja	Moderada	Moderada	Alta	Extrema
	1	Baja	Baja	Moderada	Alta	Extrema

Fuente: Elaboración propia a partir de la Guía para la administración del riesgo y el diseño de controles en Entidades públicas del DAFP (2020)

Riesgo después de controles. Una vez identificado el riesgo inherente, se debe realizar la identificación de controles y posteriormente su valoración mediante la evaluación del diseño y ejecución de estos, lo cual genera como resultado el riesgo residual. Lo ideal es que por cada causa se identifique el control o controles existente.

Identificación de Controles. La definición de controles para que en su diseño mitiguen de manera adecuada el riesgo (causas), depende de varios aspectos: las características propias del proceso y las actividades relacionadas con el riesgo, la variable determinante del riesgo (frecuencia o impacto), las vulnerabilidades identificadas, entre otros. Los controles deben contribuir a la afectación de la probabilidad o el impacto y deben estar acordes con las causas y consecuencias identificadas.

Tipología de controles y los procesos: a través del ciclo de los procesos es posible establecer cuándo se activa un control y, por lo tanto, establecer su tipología con mayor precisión. Para comprender esta estructura conceptual, en la ilustración 2 se consideran 3 fases globales del ciclo de un proceso así:

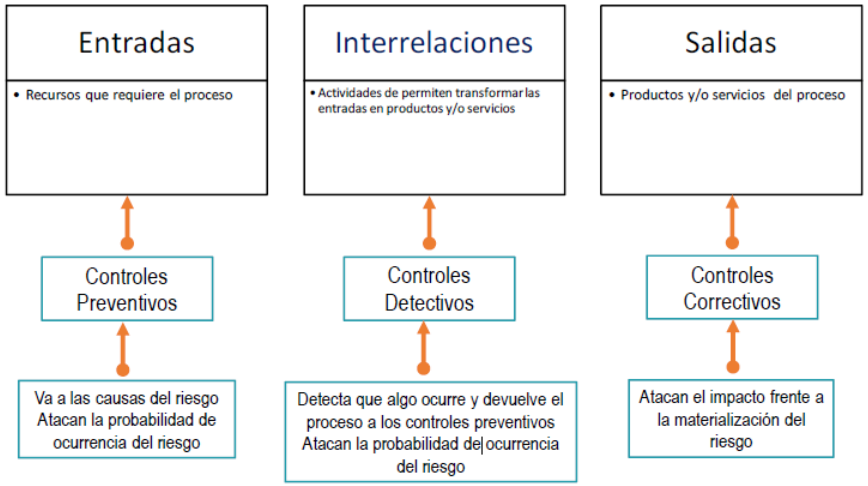

Ilustración 2: Ciclo de proceso y tipologías de controles

Fuente: Tomada de la Guía para la administración del riesgo y el diseño de controles en Entidades públicas del DAFP (2020)

Acorde con lo anterior, tenemos las siguientes tipologías de controles:

- Control preventivo: control accionado en la entrada del proceso o antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado, por lo que su objetivo es asegurar o garantizar (verbos sugeridos para su redacción). Esta tipología ataca la probabilidad del riesgo.
- Control detectivo: control accionado durante la ejecución del proceso o la actividad generadora del riesgo. Estos controles detectan el riesgo, pero generan reprocesos; se aseguran por tener como objetivo validar o verificar (verbos sugeridos para su redacción). Esta tipología ataca la probabilidad del riesgo.

- Control correctivo: control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos y ataca el impacto del riesgo.

Así mismo, de acuerdo con la forma como se ejecutan tenemos:

- Control manual: controles que son ejecutados por personas.
- Control automático: son ejecutados por un sistema.

- **Valoración de controles***:* Al momento de definir las actividades de control por parte de la primera línea de defensa se debe considerar que los controles estén bien diseñados, es decir, que efectivamente mitiguen las causas que hacen que el riesgo se materialice, y se ejecuten adecuadamente.
- **Nivel de riesgo (riesgo residual***)*. Dado que ningún riesgo se evita o elimina mediante una medida de tratamiento, el desplazamiento de un riesgo inherente en su probabilidad o impacto se realizará de acuerdo con la valoración del control (fuerte, moderado, débil) y el objeto del mismo (disminuir probabilidad o impacto) moviéndose dentro de la matriz de calor, cuyo resultado será el riesgo residual el cual deberá ser tratado.

Nota: En el caso que un riesgo no tenga controles diseñados, es deber del líder de proceso, gerente de meta o según aplique, diseñar y ejecutar un control en el menor tiempo posible en el marco del plan de tratamiento, para que posterior a la finalización de la actividad, se vuelva a valorar el riesgo, pero con el control incluido, de tal manera que se afecte la zona residual.

4. **Tratamiento (manejo).** En esta etapa se formulan las acciones orientadas al mejoramiento de los controles o de implementación de nuevos controles, de acuerdo con el nivel residual y los niveles de aceptación definidos en esta política de gestión del riesgo, es decir, el tratamiento de los riesgos parte del nivel de aceptación de la política de gestión de riesgos de FONCEP, la cual establece:

   "los riesgos en niveles de exposición "moderado", alto" o "extremo" son inaceptables y deberán ser tratados de acuerdo con alguna de las opciones de manejo establecidas (evitar, reducir o compartir el riesgo). Los riesgos de corrupción son inaceptables, independientemente de su nivel y deben ser tratados."

Por sus criterios de probabilidad e impacto, los riesgos de corrupción nunca estarán en un nivel de riesgo inherente ni residual bajo.

De acuerdo con las disposiciones de la Alta Dirección, los niveles de aceptación de los riesgos del FONCEP son los que se encuentran en la zona de riesgo baja, para los riesgos que se encuentran en la zona de riesgo moderada, zona de riesgo alta y zona de riesgo extrema los planes de tratamiento de riesgos son obligatorios.

Tabla 10: Zonas de riesgo y Plan de tratamiento

Zona de riesgo	Plan de tratamiento
Extrema	Si
Alta	Si
Moderada	Si
Baja	No

Fuente: Elaboración propia.

De acuerdo con el nivel de exposición en que se encuentre cada riesgo y la relación costo-beneficio de las medidas de tratamiento, se define la opción de manejo a aplicar. Las opciones de tratamiento son:

- Aceptar el riesgo: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (ningún riesgo de corrupción podrá ser aceptado).
- Evitar el riesgo: Se abandonan las actividades que dan lugar al riesgo, es decir, no se inicia o no se continúa con la actividad que lo provoca.
- Reducir el riesgo: Se adoptan medidas para reducir la probabilidad o el impacto del riesgo o ambos; por lo general conlleva la implementación de controles.
- Compartir o transferir el riesgo: Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad.

Nota: Solo se puede seleccionar una opción de tratamiento.

Estas acciones deben estar encaminadas a: fortalecer el diseño de los controles existentes; realizar monitoreo y revisión a la efectividad de los controles existentes; crear nuevos controles asociados al riesgo.

5. **Monitoreo y revisión.** Es la revisión periódica de la eficacia de las acciones de tratamiento y los controles que se han implementado, así como la materialización de los riesgos. El monitoreo de los riesgos se realiza por medio de las tres líneas de defensa con el fin de asegurar el logro de sus objetivos, de esta manera se proporciona el aseguramiento de la gestión y se previene la materialización de los riesgos en todos sus ámbitos

Tabla 11: Líneas de defensa y Responsabilidades de Monitoreo

Líneas de defensa	Responsabilidades de monitoreo
Línea estratégica	La alta dirección y el equipo directivo, a través de sus comités (Comités Institucional de Coordinación de Control Interno, Comité de Gestión y Desempeño) o de la Junta Directiva deben monitorear y revisar el cumplimiento a los objetivos a través de una adecuada gestión de riesgos en relación con lo siguiente: • Revisar los cambios en el direccionamiento estratégico y determinar cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados. • Revisar el adecuado despliegue de los objetivos institucionales en los objetivos de procesos que han servido de base para llevar a cabo la identificación de los riesgos. • Hacer seguimiento en el Comité Institucional y de Control Interno a la implementación de cada una de las etapas de la gestión del riesgo y de los resultados de las evaluaciones realizadas por Control Interno o Auditoría Interna. • Revisar el cumplimiento a los objetivos institucionales y de procesos y sus indicadores e identificar, en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos. • Hacer seguimiento y pronunciarse, por lo menos cada trimestre, sobre el perfil de riesgo inherente y residual de la Entidad, incluyendo los riesgos de corrupción y de acuerdo con las políticas de tolerancia establecidas y aprobadas. • Revisar los informes presentados por la segunda y tercera línea de defensa, por lo menos cada trimestre, de los eventos de riesgos que se han materializado en la Entidad, incluyendo tanto los riesgos de corrupción, como las causas que dieron origen a esos eventos de riesgos materializados, y de aquellas que están ocasionando que no se cumplan los objetivos y metas, a través del análisis de indicadores asociados a esos objetivos. • Revisar las actividades/acciones de mejoramiento establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento.
Primera línea de defensa	• Revisar los cambios en el direccionamiento estratégico y como estos puedan generar nuevos riesgos o modificar los que ya se tienen. • Revisar el adecuado diseño y ejecución de los controles. • Revisar que las actividades de control de sus procesos estén documentadas y actualizadas en los procedimientos, manuales o documentos oficiales del Sistema de Gestión del FONCEP. • Revisar el cumplimiento de objetivos de procesos, indicadores de desempeño, metas estratégicas, seguridad de los activos de información, objetos contractuales y los objetivos de los sistemas de gestión de la Entidad, identificando los riesgos cuando estos elementos no se estén cumpliendo.

Líneas de defensa	Responsabilidades de monitoreo
	• Reportar a la segunda línea de defensa los eventos de riesgo que se han materializado en la Entidad, así como las causas que dieron origen a esos eventos. • Revisar los planes de mejoramiento de las auditorias, garantizando la identificación de la o las causas raíz, de tal forma que se evite la repetición de los eventos y del riesgo en general. • Ejecutar las actividades y planes de acción acordados de las líneas de defensa relacionados con la gestión del riesgo. • Revisar constantemente los riesgos y el adecuado diseño y ejecución de los controles establecidos. • Revisar que las actividades de control se encuentren documentadas y actualizadas en los procedimientos o documentos oficiales del Sistema de Gestión del FONCEP. • **Cada vez que se incumpla objetivos, indicadores o se tenga hallazgos de auditoría, se debe identificar o valorar los riesgos del proceso y proponer acciones de mejora y de tratamiento.** • Reportar a la segunda línea de defensa los riesgos materializados (provenientes de procesos de autoevaluación, auditorías) según lo dispongan. • Ejecutar los controles y actualizarlos cuando se requiera, además de generar reportes de monitoreo y reportar evidencias cuando las demás líneas de defensa así lo requieran.
Segunda línea de defensa	• Revisar los cambios en el direccionamiento estratégico y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen, con el fin de solicitar y apoyar en la actualización de las matrices del riesgo. • Revisar la adecuada definición y despliegue de los objetivos institucionales a los objetivos de los procesos; de las metas estratégicas a los indicadores estratégicos, acciones de los planes y objetos contractuales; de los objetos contractuales a las obligaciones contractuales que han servido de base para llevar a cabo la identificación de los riesgos, y formular las recomendaciones a que haya lugar. • Revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han identificado por parte de la primera línea de defensa y determinar las recomendaciones y seguimiento para el fortalecimiento de los primeros. • Revisar el perfil de riesgo inherente y residual por cada proceso, consolidarlo y pronunciarse sobre cualquier riesgo que esté por fuera del perfil de riesgo de la Entidad. • Hacer seguimiento a las actividades de control establecidas para la mitigación de los riesgos de los procesos, verificando que se encuentren documentadas y actualizadas en los procedimientos o documentos oficiales del Sistema de Gestión del FONCEP. • Revisar las acciones de mejoramiento y tratamiento establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelva a materializar

Líneas de defensa	Responsabilidades de monitoreo
	el riesgo y lograr el cumplimiento a los objetivos, metas, planes, indicadores, objetos contractuales y objetivos de sistemas de gestión. • Trimestralmente los responsables de segunda línea de defensa deben realizar un informe en el que se incluyan los elementos susceptibles a mejorar por cada una de la tipología de riesgos a su cargo, dando a conocer las acciones (plan de acción) a realizar por la primera línea de defensa: Como elementos mínimos a incluir en el informe este debe tener: acciones realizadas durante el trimestre, acciones a realizar en el próximo trimestre, estado de los riesgos (cantidad, nivel de riesgo residual, riesgos materializados), estado de causas, diseño y ejecución de controles, cumplimiento de plan o acciones de tratamiento y finalmente se debe identificar debilidades y oportunidades de la gestión de riesgos de las primeras líneas de defensa a intervenir.
Tercera línea de defensa	• Revisar los cambios en el direccionamiento estratégico o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de identificar y actualizar las matrices de riesgos por parte de los responsables. • Revisar la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos; de las metas estratégicas a los indicadores estratégicos, acciones de los planes y objetos contractuales; de los objetos contractuales a las obligaciones contractuales que han servido de base para llevar a cabo la identificación de los riesgos y realizar las recomendaciones a que haya lugar. • Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos e incluir los riesgos de corrupción. • Revisar el adecuado diseño y ejecución de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y formular las recomendaciones y seguimiento para el fortalecimiento los controles. • Revisar el perfil de riesgo inherente y residual consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la Entidad o que su calificación del impacto o probabilidad del riesgo no es coherente con los resultados de las auditorías realizadas. • Realizar auditorías para verificar que las actividades de control establecidas con el fin de mitigar los riesgos, se encuentren documentadas y actualizadas en los procedimientos, además, que los planes de mejora de hallazgos se lleven a cabo de manera oportuna, se establezcan las causas raíz del problema y se evite, en lo posible, la repetición de hallazgos y la materialización de los riesgos.

Fuente: Elaboración propia a partir de la información de la Guía para la administración del riesgo y el diseño de controles en Entidades públicas del DAFP (2020)

Nota: En los siguientes capítulos se desarrollan las particularidades de cada una de las tipologías de riesgos. Para los riesgos que no cuentan con particularidades, se deberán cumplir los lineamientos descritos en los capítulos anteriores.

IV. CAPÍTULO 4. RIESGOS DE METAS Y RESULTADOS, DE CORRUPCIÓN Y DE PROCESO

Este apartado tiene como fin establecer las particularidades de los riesgos estratégicos, de corrupción y de proceso. Como se mencionó en el apartado de generalidades estos tipos de riesgos estarán coordinados por la Oficina Asesora de Planeación.

a) Identificación. Una vez definido el contexto, ya sea mediante los espacios definidos como Comité Institucional de Gestión y Desempeño, Comités Directivos, los ejercicios de planeación, los Comités Primarios o ejercicios de análisis de los procesos, se procede con la identificación o descripción del riesgo. Esta identificación se lleva a cabo determinando las causas con base en el contexto interno, el contexto externo y del proceso que pueden afectar el logro de los objetivos. Es decir, esta fase está asociada a la descripción de aquellos eventos o situaciones que pueden entorpecer el normal desarrollo de los objetivos del proceso que depende de la tipología.

Orientación para la identificación del riesgo

- ✓ Al momento de identificar riesgos, tenga en cuenta la información de fuentes como hallazgos de auditorías, PQRS, directrices o intereses de la alta dirección (actas de comités), procesos de autoevaluación, datos históricos, experiencia del equipo de trabajo, entre otros.
- ✓ Al momento de identificar y analizar las causas, tenga en cuenta que los objetivos del proceso o de meta estratégica se desarrollan a través de actividades y que no todas tienen la misma importancia. Por esa razón, se debe establecer cuál de ellas contribuyen mayormente al logro de los objetivos, estas actividades se denominan *actividades críticas o factores claves de éxito.* Son estos factores los que se deben tener en cuenta para identificar las causas que originan la materialización de los riesgos. Por lo anterior, las caracterizaciones de los procesos y los planes de acción son el insumo fundamental y por ende deben ser coherentes y estar actualizados.
- ✓ En la identificación de causas, estas deben estar asociadas a por lo menos alguno de los 5 factores generadores establecidos: proceso, talento humano, tecnología, infraestructura, o evento externo.
- ✓ Al momento de definir efecto o impacto, tenga en cuenta la *Tabla 8. Criterios para calificar el impacto*.

Buenas prácticas para identificar riesgos:

- ✓ Antes de iniciar la identificación, es indispensable actualizar la documentación como caracterizaciones y procedimientos, específicamente objetivos, actividades y explicaciones específicas de estos documentos que den a conocer la realidad de la gestión; lo anterior, porque en muchos casos la documentación permanece igual, aun cuando en una Entidad no es estática y existen avances constantes y permanente en el día a día del cómo se realizan las actividades.
- ✓ Analizar el objetivo del proceso el cual se encuentra en la caracterización
- ✓ Priorizar actividades del "hacer" del ciclo PHVA de la caracterización, pues es la razón del ser del proceso, analizando entradas y salidas.
- ✓ Analizar metas estratégicas, específicamente las actividades críticas y de éxito para alcanzarla.
- ✓ Analizar y revisar los indicadores o métricas en todos los niveles (estratégico, de proceso etc.)
- ✓ Revisar las auditorias del último año, específicamente hallazgos y recomendaciones.
- ✓ Realizar mesas de trabajo al interior de las dependencias para que el capital humano con más trayectoria de a conocer los sucesos por los cuales ha pasado el proceso.
- ✓ Revisar matrices de riesgos de Entidades similares o del sector para identificar factores similares.
- ✓ **El nombre del riesgo debe tener sustantivo + verbo en participio + adjetivo , adverbio o complemento negativo**

Ejemplo: Procesos coactivos en contra de FONCEP defendidos inadecuadamente, Cuotas partes cobradas fuera de tiempo o del mandato, Cartera hipotecaria del FAVIDI recaudada de manera ineficiente

Identificar las causas: establezca la siguiente estructura **causa + agente generador + cuándo o cómo**

Identificar impacto: el proceso o área debe identificar la consecuencia a la cual se ve expuesta la organización en caso de materializar un riesgo.

Las preguntas claves para la identificación del riesgo permiten determinar:

- ¿Qué puede suceder? (Riesgo) Identificar la afectación del cumplimiento del objetivo estratégico, meta o del proceso según sea el caso.
- ¿Cómo y cuándo puede suceder y qué o quién lo puede generar? (Causas) Establecer las causas a partir de los factores determinados en el contexto.
- ¿Qué consecuencias tendría su materialización? (Impacto) determinar los posibles efectos por la materialización del riesgo.

Nota: A partir de la respuesta de estas preguntas se debe describir el riesgo.

Ejemplo

Tabla 12: Riesgo – Causas – Impacto/Efecto

Nombre del riesgo	Causas	Impacto/ Efecto
Seguimiento de depuración a deudas distritales realizado parcialmente	• Participación intermitente o nula por parte de los entes que hacen parte de la depuración de deuda durante cada mes. • Realización de actividades de seguimiento de manera inoportuna por parte del equipo del proceso de Administración de Historias Laborales en el momento que se allegan los estados de cuenta.	• Identificación de desviaciones, inconsistencias, incumplimientos de las actividades del proceso • Si representa hasta el 4% del presupuesto de funcionamiento asignado en la vigencia • Incumplimiento de salidas de procesos o Incumplimiento del Plan de Acción Institucional • Imagen institucional afectada entre los grupos de valor de FONCEP

Fuente: Elaboración propia.

Riesgos de corrupción: para identificar estos riesgos es necesario revisar la definición de este tipo de riesgo en la parte de definiciones, pues al momento de describirlo es necesario que en la descripción concurran los componentes de su definición así: acción u omisión + uso del poder + desviación de la gestión de lo público + beneficio privado.

Nota: Los riesgos de corrupción se identifican o valoran anualmente por los responsables de los procesos, y la OAP consolida los riesgos de corrupción y pública el mapa de corrupción en el marco del Plan Anticorrupción y Atención al Ciudadano PAAC en la página web de la Entidad (enlace de transparencia) a más tardar el 31 de enero de cada año teniendo en cuenta el índice de información clasificada y reservada.

Ejemplo

Tabla 13: Riesgo – Causas – Impacto/Efecto

Nombre del riesgo	Causas	Impacto/ Efecto
Posibilidad de recibir una dádiva o beneficio a nombre propio o de un	• Ausencia o debilidades de controles para la verificación de requisitos por parte del área de	• Imagen institucional afectada entre

tercero al nombrar o vincular personal sin cumplimiento de requisitos legales establecidos en el manual de funciones vigente.	talento humano en el procedimiento vinculación de servidores. • Desconocimiento del procedimiento vinculación de servidores por parte del equipo del área al iniciar una nueva vinculación	los grupos de valor de FONCEP. Inicio de investigación disciplinaria a servidores del FONCEP • Sanciones disciplinarias, fiscales y/o penales que impidan el cumplimiento del plan de acción institucional

Fuente: Elaboración propia.

b) Análisis. En este punto se define la probabilidad y el impacto como se mencionó en el capítulo del ciclo de riesgos. Tener en cuenta lo establecido en las tablas 6 , y y 8 respecto a los criterios para definir la probabilidad y el impacto.

c) Evaluación y valoración. Una vez se tiene el riesgo inherente, se debe iniciar la identificación y valoración de los controles

Orientaciones técnicas para la identificación de controles:

- ✓ Para la identificación de controles es necesario describir adecuadamente las causas como se mencionó en el capítulo anterior. Con una causa bien descrita (causa + agente generador + cuándo o cómo) se facilita la identificación de controles.
  Ejemplo
  Si hay una causa denominada "*Ausencia o debilidad de controles para la verificación de requisitos por parte del área de talento humano en el procedimiento vinculación de servidores"*, lo ideal es crear controles que se ejecuten antes o durante la ejecución del procedimiento mencionado, pues es ahí donde se puede detectar la causa; si se hace posteriormente, puede que el control no sea efectivo o solo detecte la materialización de una causa.
- ✓ El ideal es que todas las causas de riesgos tengan por lo menos un control; de no ser así, se debe velar porque en los tratamientos se llegue a tener uno.
- ✓ Los controles pueden ser de tres clases: **preventivos, detectivos y correctivos** como se dijo en el capítulo anterior. Se recomienda que los controles se orienten a la prevención y no a la detección de causas.

- ✓ Los controles preventivos y detectivos afectan la probabilidad y los correctivos el impacto. En ningún caso un control puede atacar la probabilidad e impacto al mismo tiempo
- ✓ Para la descripción del control tenga en cuenta que en su redacción debe tener las siguientes variables:
    - Responsable de llevar a cabo el control: persona asignada para ejecutar el control, el cual debe tener autoridad, competencias y conocimientos para ejecutarlo (el profesional, el auxiliar, el líder u otras personas).
    - Periodicidad de ejecución: debe contener una periodicidad específica para su realización (diario, mensual, trimestral, anual, cada vez que sea necesario.). En todo caso la ejecución del control debe ser oportuna para mitigar el riesgo.
    - Propósito: se debe indicar para qué se realiza el control, este debe prevenir o detectar las causas que generan el riesgo (verificar, validar, conciliar, comparar, revisar, cotejar, detectar, identificar y acciones semejantes).
    - Cómo se realiza la actividad del control: se debe indicar el cómo se realiza la actividad determinando si la fuente u orden de la información que sirve para ejecutar el control es confiable para mitigar el riesgo (a través de, identificando, comparando y acciones semejantes)
    - Qué pasa con las observaciones o desviaciones: El control debe indicar qué pasa con las observaciones o desviaciones como resultado de la ejecución del control, es decir, si se encuentran diferencias o no se cumple el control en su totalidad, la actividad no debería continuar hasta subsanar el hecho (en preventivos), o debería gestionarse la materialización de la causa o riesgo de manera oportuna con acciones correctivas o aclaraciones a las diferencias detectadas.
    - Evidencia: Debe indicar cual es el producto para entregar como evidencia de ejecución del control. Es necesario en la medida de lo posible definir donde reposará las evidencias de ejecución del control.

Ejemplo

Tabla 14: Causas – Control

Causa	Control

Información inoportuna e insuficiente por parte de la Gerencia de Bonos y Cuotas partes, tesorería y/o gestión documental para dar respuesta a los mandamientos de pago notificados a FONCEP	El Abogado de defensa de cobro coactivo, cada vez que requiera información de otras áreas para dar respuesta al mandamiento de pago, garantiza informar las **características y tiempos de envío de información** mediante una comunicación interna al área pertinente por medio del aplicativo SIGEF. En caso de no obtener la información requerida en los términos señalados, el abogado encargado de la defensa presentará la excepción de falta de título ejecutivo a fin de obtener nueva información por parte de la gerencia de bonos y/o áreas involucradas que será incorporada posteriormente al recurso de reposición. La evidencia de este control son las comunicaciones internas radicadas por el abogado de la defensa del área de cobro coactivo.

Fuente: Elaboración propia.

Nota: El control se debe iniciar con un cargo responsable o un sistema o aplicación evitando asignar áreas de manera general o nombres de personas. El control debe estar asignado a un cargo específico o comité cuando aplique.

Orientaciones técnicas para valoración de controles:

- ✓ Para la adecuada mitigación de los riesgos no basta que control esté bien diseñado, el control debe ejecutarse por parte de los responsables tal como se diseñó. Un control que no se ejecute o un control que se ejecute y esté mal diseñado, no va a contribuir a la mitigación del riesgo.
- ✓ Hay dos (2) criterios clave para evaluar controles, el tipo de control (preventivo, detectivo y correctivo) y la implementación, es decir, la forma de ejecutarlo (automático y manual). Hay otros criterios para el diseño de los controles los cuáles no se consideran cuantitativamente para evaluar su efectividad, pero refuerzan su diseño, estos criterios se consideran como atributos informativos y corresponden a la documentación, evidencia y frecuencia de aplicación:

  Tipo:

  - Preventivo: Va hacia las causas del riesgo, aseguran el resultado final esperado.
  - Detectivo: Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.
  - Correctivo: Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.

  Implementación:

  - Automático: Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.

- Manual: Controles que son ejecutados por una persona, tiene implícito el error humano.

Documentación:

- Documentado: Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso que corresponda a oficiales del Sistema de Gestión del FONCEP.
- Sin documentar: Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso.

Frecuencia:

- Continua: El control se aplica siempre que se realiza la actividad que conlleva el riesgo.
- Aleatorio: El control se aplica aleatoriamente a la actividad que conlleva el riesgo.

Evidencia:

- Con registro: El control deja un registro permite evidencia la ejecución del control.
- Sin registro: El control no deja registro de la ejecución del control.

✓ Adicionalmente, FONCEP cuenta preguntas complementarias que buscan orientar para el diseño de controles efectivos:

- Responsable: ¿Existe un responsable asignado; este tiene autoridad y funciones en la ejecución del control?
- Periodicidad: ¿Es oportuna la ejecución del control para detectar o prevenir la mitigación del riesgo?
- Propósito: ¿Las actividades buscan prevenir o detectar las causas?
- Confiabilidad: ¿La fuente de información que se utiliza en el desarrollo del control es información confiable?
- Manejo de las observaciones o desviaciones: ¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?
- Evidencia de la ejecución del control: ¿Se deja evidencia o rastro de la ejecución del control que permita a cualquier tercero con la evidencia llegar a la misma conclusión?
- Efecto del control: ¿El resultado de cada variable de diseño del control, a excepción de la evidencia, va a afectar la calificación del diseño del control? Esto debido a que deben intervenir en el control todas las variables para que el control se evalúe como bien diseñado, generando de esta forma una calificación entre fuerte, moderado o débil.

- ✓ Mitigación del riesgo: Los controles, además de estar bien diseñados, deben ejecutarse de manera consistente, de tal forma que se pueda mitigar el riesgo. Esto implica que la primera línea de defensa debe asegurar que se ejecuten los controles. Por tal razón el responsable del proceso debe confirmar la ejecución del control, que será nuevamente confirmada mediante la evaluación de la OCI. Esta evaluación también se expresa en términos de fuerte, moderado y débil, evaluaciones relacionadas con la ejecución consistente, algunas veces o no se ejecuta del todo.

Nota: En el caso que un riesgo no tenga controles diseñados, es deber del líder de proceso, gerente de meta o según aplique, diseñar y ejecutar un control en el menor tiempo posible en el marco del plan de tratamiento, para que posterior a la finalización de la actividad, se vuelva a valorar el riesgo, pero con el control incluido, de tal manera que se afecte la zona residual.

Plan de contingencia. Se entiende como el conjunto de medidas que se definen en la identificación del riesgo y que se deben ejecutar en caso de que se materialice el riesgo. Por tal razón, solo hasta la materialización del riesgo se debe ejecutar. **Los Riesgos que deben describir las acciones de contingencia son los aquellos cuyo nivel de riesgo residual sea extremo.**

Nota: los riesgos cuya acción de tratamiento sea aceptarlos, solo pueden ser definidos previa autorización de la alta dirección en los escenarios definidos.

d) Tratamiento (manejo)

En este paso se debe incluir y asociar las acciones de tratamiento, las cuales deben estar en el Plan de Acción Institucional, que se van a realizar en la vigencia, según lo establecido en la política de riesgos.

e) Monitoreo

Los responsables de los riesgos deben revisar trimestralmente el estado de los mismos, causas, controles y tratamiento a través del aplicativo SVE. La OAP establecerá los periodos de reporte de esta revisión y las modificaciones a las que haya lugar.

La segunda línea de defensa de estos riesgos (OAP, OIS, GTH, SFA) garantizarán la veracidad del monitoreo mediante la revisión de la información observando el estado del propio riesgo, controles, y acciones de tratamiento. Las segundas líneas de defensa deben formular recomendaciones y observaciones a la primera línea de defensa.

El monitoreo de riesgos se evidenciará en el informe de riesgos de la segunda línea de defensa, el cual se realiza trimestralmente y se socializa en el Comité Institucional de Gestión y Desempeño; este informe incluye el estado de riesgos trimestralmente, incluyendo: número de riesgos, nivel residual,

estado de acciones de tratamiento, materializaciones en el último trimestre, acciones realizadas y a realizar sobre la gestión del riesgo, además de incluir aquella información solicitada por los grupos de interés. También el informe de las líneas de defensa es consolidado por la OAP y publicado en el espacio dispuesto para esto con el fin que las partes interesadas conozcan el mismo.

Seguimiento de riesgos de corrupción. El Jefe de Control Interno es el responsable de adelantar seguimiento al Mapa de Riesgos de Corrupción. En este sentido es necesario que lleve a cabo el seguimiento a la gestión del riesgo verificando la efectividad de los controles con corte a los días 30 de los meses de abril, agosto y diciembre. En esa medida la publicación deberá surtirse dentro de los diez (10) primeros días de los meses siguientes en la página web de la Entidad o en un lugar de fácil acceso para la ciudadanía.

El seguimiento a la gestión de riesgos en sus diferentes tipologías se realizará según lo establecido y aprobado en el plan anual de auditoría aprobado por el Comité Institucional de Coordinación de Control Interno.

Este tipo de seguimiento comprendelas siguientes actividades:

- Verificación de la publicación del Mapa de Riesgos de Corrupción en la página web de la Entidad.
- Seguimiento a la gestión del riesgo.
- Revisión de los riesgos y su evolución.
- Aseguramiento de que los controles sean efectivos, apunten al riesgo y estén funcionando en forma adecuada.

f) Materialización de riesgos

Hace relación a hechos que identificados o no como riesgos, generan un impacto negativo en los objetivos de proceso o de la Entidad. Estos se pueden observar directamente mediante hallazgos de auditorías, pero también de insumos como PQRS constantes, procesos de autoevaluación y otros análogos.
En todo caso, cada vez que ocurra una materialización de riesgos la primera línea de defensa debe realizar los siguientes pasos 🔍:

- Informar a la segunda línea de defensa la materialización del riesgo.
- Si el riesgo tiene plan de contingencia, ejecutarlo, de lo contrario crear uno y aplicarlo.
- Realizar el análisis de causas y formulación de acciones según Manual para el análisis de causas y formulación de acciones/actividades preventivas, correctivas y de mejora MOI-EST-MIP-007 y el Formato solicitudes de modificación al plan de acción y análisis de causa FOR-EST-MIP-027. Debe surtir el efecto de inclusión de actividades o modificación del PAI, según el Manual para la formulación y seguimiento del plan de acción institucional MOI-EST-PES-003.

- Posterior a realizar el análisis de causas y de solicitar la creación de las actividades en plan de acción institucional, registrar la materialización en el aplicativo SVE identificando información solicitada por el sistema. Tenga en cuenta que la información del formato de análisis de causas es el insumo para registrar la información en SVE en la materialización.
- Si resultado del análisis de causas así se define, identificar o evaluar nuevamente el riesgo o crear el riesgo (si no había sido identificado) en el aplicativo SVE realizando todo el ciclo de gestión.
- Socializar el plan de mejoramiento y materialización de riesgos en comité primario y en espacios directivos (comité de la dirección, Comité Institucional del Coordinación de Control Interno-CICCI, Comité Institucional de Gestión y Desempeño-CIGD, o junta directiva etc.). En caso de generarse observaciones por parte de los integrantes del comité, agregar las acciones al plan de mejoramiento.

g) Comunicación y consulta

Las actividades de comunicación y consulta con los grupos de valor tienen lugar durante todas las etapas del proceso para la gestión del riesgo, estas actividades están dadas por:

- El mapa de riesgos que deberá ser divulgado para consulta al interior de la Entidad.
- Los líderes y responsables de cada riesgo deben divulgar y sensibilizar al interior de sus dependencias el mapa de riesgos junto con las acciones asociadas para su mitigación (acciones de tratamiento)
- La Oficina Asesora de Planeación y la Oficina de Control Interno, impulsarán a nivel institucional una cultura de gestión del riesgo, a través de capacitaciones, mesas de trabajo y asesorías con el fin de mejorar el conocimiento y apropiación del enfoque basado en riesgos.
- Las acciones de tratamiento de los riesgos priorizados que involucren partes interesadas o terceros serán divulgadas por parte de los líderes y responsables de cada riesgo.
- La consolidación del mapa de riesgos de corrupción, proceso, estratégicos, seguridad de la información, ambientales, Seguridad y Salud en el Trabajo le corresponde realizarla a la Oficina Asesora de Planeación, que hará las veces de facilitador del ciclo de Gestión de Riesgos en las dependencias.
- La consulta y divulgación del Mapa de Riesgos de Corrupción a partes interesadas y comunidad en general se realizará a través de su publicación en la página Web en el enlace de transparencia.
- La Política de Gestión de Riesgos y demás aspectos metodológicos del presente manual deberán ser divulgados a funcionarios y contratistas del FONCEP mínimo una vez en cada vigencia administrativa por parte de la Oficina Asesora de Planeación y la Oficina de Control Interno.
- El mapa de riesgos deberá ser socializado a las partes interesadas por parte de la segunda línea de defensa. Se recomienda que esta acción se realice mediante la publicación del informe en la página web de la Entidad.
- Publicar en el espacio asignado los informes de segunda línea de defensa.

Otras acciones:

- Cada vez que finalice las acciones de tratamiento de un riesgo se debe realizar nuevamente el análisis y la evaluación de este, o cuando el proceso o la segunda línea de defensa lo establezca.
- Todo hallazgo de auditoría interna y externa, PQRS contantes, o incumplimiento de indicadores o metas debe tener un impacto en riesgos (ya sea en el riesgo, causas, controles o acciones de tratamiento) de tal forma que el líder del proceso debe actualizar el riesgo.

V. CAPÍTULO 5. RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

A medida que las redes interconectan y los flujos de los datos son libres, se vuelve muy importante permitir que estas proporcionen servicios de seguridad. En el mundo, la conectividad ya no es opcional y los posibles riesgos de dicha conectividad, que implican flujos de información de todo tipo, deben ser protegidas. Para proveer una adecuada protección a los recursos de la infraestructura de red, los procedimientos y tecnologías que se despliega deben garantizar tres cosas:

- **Confidencialidad:** Garantía de que la información personal será protegida para que no sea divulgada sin consentimiento de la persona. Dicha garantía se lleva a cabo por medio de un grupo de reglas que limitan el acceso a esta información, garantizando que solo los usuarios autorizados puedan acceder a esta.
- **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso, es decir, la información se conserva en su versión original y garantiza que solo las personas autorizadas pueden usar esta información.
- **Disponibilidad del sistema y de la información:** Es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

Este apartado tiene como fin establecer las particularidades de los riesgos seguridad de la información. Como se mencionó en el apartado de generalidades estos tipos de riesgos están coordinados por la Oficina de Informática y Sistemas.

a) Identificación. Una vez definido el contexto, ya sea mediante los espacios definidos como Comité Institucional de Gestión y Desempeño, Comités Directivos, los ejercicios de planeación, los Comités Primarios o ejercicios de análisis de los procesos, se procede con la identificación o descripción del riesgo. Esta identificación se lleva a cabo determinando las causas con base en el contexto interno, el contexto externo y del proceso que pueden afectar

el logro de los objetivos. Es decir, esta fase está asociada a la descripción de aquellos eventos o situaciones que pueden entorpecer el normal desarrollo de los objetivos del proceso que depende de la tipología de seguridad de la información.

Orientación para la identificación del riesgo

- ✓ El término "seguridad de la información" contempla un conjunto de medidas preventivas y reactivas de las organizaciones y sus sistemas tecnológicos que buscan resguardar y proteger la información, esta información puede encontrase de forma física o digital.
- ✓ Al momento de identificar riesgos, tenga en cuenta la información de fuentes como hallazgos de auditorías, análisis de vulnerabilidades, pen testing, autodiagnósticos, entre otros.
- ✓ Al momento de identificar y analizar las causas, tenga en cuenta determinar el activo especifico asociado a su proceso. Por esa razón, se debe establecer cuál de ellos contribuyen en mayor medida al cumplimiento de los objetivos misionales de cada área y de la organización.
- ✓ En la identificación de causas, estas deben estar asociadas a por lo menos alguno de los 5 factores generadores establecidos: proceso, talento humano, tecnología, infraestructura, o evento externo.
- ✓ Al momento de definir efecto o impacto, tenga en cuenta la *Tabla 8. Criterios para calificar el impacto*.

Buenas prácticas para identificar riesgos

- ✓ Antes de iniciar la identificación, es indispensable actualizar la documentación de los activos disponibles en cada dependencia y/o área dentro de FONCEP.
- ✓ Analizar el activo asociado a la caracterización y relevancia que representa.
- ✓ Identificar el personal que tiene acceso a dicho activo.
- ✓ Especificar y tener un responsable o propietario del activo.
- ✓ Generar procesos de capacitación y concientización sobre los activos por dependencias y/o áreas, así como establecer la importancia de conservar la seguridad en ellos.
- ✓ Divulgar y generar campañas de socialización sobre la importancia de la seguridad en los activos.
- ✓ Revisar matrices de riesgos de Entidades similares o del sector para identificar factores similares.

Identificación del Riesgo

Se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información en cualquier activo, teniendo en cuenta que podrán combinarse de acuerdo con el análisis que realice cada dependencia y/o área:

- Pérdida de la confidencialidad.
- Pérdida de la integridad.
- Pérdida de la disponibilidad.

Para la identificación de riesgos de seguridad de la información es necesario identificar los activos de información. Cada proceso debe identificar sus activos de información como se evidencia el **Procedimiento gestión de activos PDT-APO-GST-013.**

Por lo anterior, cada riesgo se debe asociar al grupo de activos, o activos específicos del proceso dependiendo la criticidad de estos, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización, es decir, se debe tener en cuenta que los riesgos se determinan en cada proceso del área específica.

- **Un activo** es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como:

    - Servicios web
    - Hardware
    - Software
    - Información física
    - Información digital
    - Instalaciones

En caso de requerirse información adicional para entender con respecto a los activos de información, revisar el **Formato inventario de activos del FONCEP FOR-APO-GST-004**, que cuenta con notas para apoyar el diligenciamiento de este y la identificación de los activos de cada proceso.

<u>Consideraciones para determinar los riesgos de seguridad de la información:</u>

- **Nombre:** Nombre del riesgo (tener en cuenta los 3 riesgos inherentes), nombre del activo y nombre del proceso.
- **Descripción:** describa el riesgo e indique información importante para comprensión, es decir, describir si corresponde a una pérdida de la confidencialidad, integridad o disponibilidad, incluir el nombre del activo y el proceso respectivo. Específicamente delimite el alcance del riesgo o como se podría materializar operativamente hablando.

Las amenazas se agrupan en dos grandes grupos:

- Amenazas físicas: Son causas potenciales tangibles de un incidente que puede resultar en pérdida o daño en la información y en dispositivos tecnológicos. Ejemplo: robo, catástrofe natural, vandalismo, etc.
- Amenazas lógicas: Son causas potenciales intangibles de un incidente que puede resultar en daño o perdida en el software y/o aplicaciones. Ejemplos: virus, troyano, malware, hacking, etc.

Se especifica quien o que materializa la amenaza, estas pueden ser:

- Personas: Internas o externas a la organización que de manera intencional o por error puedan causar un incidente o sustracción.
- Programas y aplicaciones específicas: Cualquier tipo de software que afecte y ponga en riesgo la información y/o dispositivos.
- Catástrofes naturales o del entorno: Eventos físicos del ambiente impredecibles y/o circunstancias adheridas a esta como: humedad, temperatura y electricidad.

La determinación de las causas está clasificada así:

Perdida de la confidencialidad - activo
- Física
  - Personas – Talento humano (1)
  - Catástrofes naturales y/o del entorno – Evento externo (2)
- Lógica
  - Programas o aplicaciones específicas - Infraestructura/tecnología (3)

Causas de la pérdida de confidencialidad

- Ausencia, falta de conocimiento, y/o violación al manejo, control y supervisión de la información por parte del personal responsable del proceso constantemente. (1)
- Falta de capacitación del manejo y protección de la información por parte del personal responsable del proceso cada seis meses. (1)
- Ausencia de protección, almacenamiento y verificación adecuada de la información, que ocasione su sustracción y/o vandalismo, por parte del personal responsable del proceso constante. (1)
- Ausencia de protección e inadecuada gestión física y respuesta por parte del personal responsable del proceso ante eventos naturales (terremoto, inundación e incendios) y eventos del entorno (corto circuito, humedad y temperatura) cada vez que suceda. (2)
- Ausencia de planes de contingencia, respaldo y respuesta ante eventos naturales y/o del entorno por parte del personal responsable del proceso cada vez que suceda. (2)
- Ausencia de respaldo de la información contenida en los diferentes dispositivos de procesamiento de datos por parte del personal técnico de TI semanalmente (3)
- Falta de conocimiento que ocasiona configuraciones erradas por parte del personal que administra los diferentes dispositivos que contienen información cada vez que se realiza una nueva configuración. (3)

Perdida de la integridad - activo

- Física
  - Personas – Talento humano/procesos (4)
- Personas – Talento humano (5)

Lógica

Programas o aplicaciones específicas - Infraestructura/tecnología (6)

Causas de la pérdida de integridad

- Inadecuado diligenciamiento y manejo de los formatos por parte del personal responsable del proceso cada vez que lo use (4)
- Ausencia y revisión de planes de contingencia, procedimientos, guías y políticas en general por parte del personal responsable cada vez que se instale, actualice y modifique una aplicativo. (4)
- Falta de revisión control y seguimiento en la asignación de permisos y manejo de la información por parte del personal del proceso constantemente. (5)
- Ausencia de sistemas de información o aplicativos que faciliten los procesos de operación y/o no contengan los parámetros para validar el cumplimiento de los términos de ley verificados por el administrador de la plataforma constantemente. (6)

Perdida de la disponibilidad - activo

- Física
  - Personas – Talento humano/procesos (7)
- Lógica
  - Personas – Talento humano (8)
  - Programas o aplicaciones específicas - Infraestructura/tecnología (9)

Causas de la pérdida de disponibilidad

- Ausencia de mecanismos de monitoreo de las plataformas tecnológicas y brechas en la seguridad de la información por parte del grupo de OIS periódicamente. (7)
- Falta de plan de contingencia, políticas de almacenamiento y programas de recuperación ante desastres por parte del personal de TI, revisadas y actualizadas cada 6 meses. (7, 8)
- Inexistencia de entrenamiento y mantenimiento de los dispositivos que manejan, almacena y resguardan la información por parte del personal de TI, trimestralmente. (8)
- Mala manipulación y/o daño en el software que maneja y almacena la información, que debe ser administrada por el personal de TI constantemente (9)

Impactos asociados a las causas

- Se analiza y asocia el impacto de acuerdo Tabla 8. Criterios para calificar el impacto según le aplique al riesgo.

Ejemplo

Nombre del riesgo	Descripción	Tipo de amenaza	Materialización de la amenaza	Causa	Consecuencia/impacto
Pérdida de la integridad de los activos de información (página web e intranet) del proceso de Gestión de Comunicaciones	Hace referencia a la pérdida de la integridad de los activos de información (página web e intranet) del proceso de Gestión de Comunicaciones. Este riesgo se materializa cuando no sean cumplidos los permisos asignados, se tengan	Físicas Lógicas	Personas Personas/ Programas y/o aplicaciones específicas.	*Inadecuada definición de roles y permisos para el manejo de la página web e intranet por parte del responsable, al momento de la solicitud de asignación de permisos en GLPI a la OIS. *Inadecuada verificación de la realización de los backup por parte del responsable del proceso, relacionado con la	*Incumplimiento de indicadores de metas estratégicas. *Pérdida de información, que se recupera en su totalidad, Asignación errada de controles de acceso por parte de FONCEP en información pública, Modificaciones y/o alteraciones en los activos, cuya pérdida de exactitud y completitud conlleva

	cambios o modificaciones no autorizados, o no se conserven los históricos en los activos de información (página web e intranet) del proceso.			página web e intranet, al momento de realizar la solicitud en GLPI a la OIS. *Inadecuada verificación de la protección contra ataques cibernéticos de la página web e intranet por parte del responsable del proceso o profesional asignado, al momento de realizar la solicitud en GLPI a la OIS.	un impacto no significativo para la entidad o entes externos. *Imagen institucional afectada entre los grupos de valor de FONCEP. *Inicio de investigación disciplinaria a servidores del FONCEP. *Sanciones disciplinarias, fiscales y/o penales que impidan el cumplimiento del plan de acción institucional

b) Análisis. En este punto se define la probabilidad y el impacto como se mencionó en el capítulo del ciclo de riesgos. Tener en cuenta las tablas 6, 7 y 8 sobre los criterios para definir la probabilidad y el impacto.

c) Evaluación y valoración. Una vez se tiene el riesgo inherente, se debe iniciar la identificación y valoración de los controles

Orientaciones técnicas para la identificación de controles:

- ✓ Para la identificación de controles es necesario describir adecuadamente las causas como se mencionó en el capítulo anterior. Con una causa bien descrita (causa + agente generador + cuándo o cómo) se facilita la identificación de controles.

  Ejemplo

  Si hay una causa denominada "Inadecuada definición de roles y permisos para el manejo de la página web e intranet por parte del responsable, al momento de la solicitud de asignación de permisos en GLPI a la OIS.", lo ideal es crear controles que se ejecuten antes o durante la ejecución del procedimiento mencionado, pues es ahí donde se puede detectar la causa; si se hace posteriormente, puede que el control no sea efectivo o solo detecte la materialización de una causa.
- ✓ El ideal es que todas las causas de riesgos tengan por lo menos un control; de no ser así, se debe velar porque en los tratamientos se llegue a tener uno.

- ✓ Los controles pueden ser de tres clases: **preventivos, detectivos y correctivos** como se dijo en el capítulo anterior. Se recomienda que los controles se orienten a la prevención y no a la detección de causas.
- ✓ Los controles preventivos y detectivos afectan la probabilidad y los correctivos el impacto. En ningún caso un control puede atacar la probabilidad e impacto al mismo tiempo
- ✓ Para la descripción del control tenga en cuenta que en su redacción debe tener las siguientes variables:
    - Responsable de llevar a cabo el control: persona asignada para ejecutar el control, el cual debe tener autoridad, competencias y conocimientos para ejecutarlo (el profesional, el auxiliar, el líder u otras personas).
    - Periodicidad de ejecución: debe contener una periodicidad específica para su realización (diario, mensual, trimestral, anual, cada vez que sea necesario.). En todo caso la ejecución del control debe ser oportuna para mitigar el riesgo.
    - Propósito: se debe indicar para qué se realiza el control, este debe prevenir o detectar las causas que generan el riesgo (verificar, validar, conciliar, comparar, revisar, cotejar, detectar, identificar y acciones semejantes).
    - Cómo se realiza la actividad del control: se debe indicar el cómo se realiza la actividad determinando si la fuente u orden de la información que sirve para ejecutar el control es confiable para mitigar el riesgo (a través de, identificando, comparando y acciones semejantes)
    - Qué pasa con las observaciones o desviaciones: El control debe indicar qué pasa con las observaciones o desviaciones como resultado de la ejecución del control, es decir, si se encuentran diferencias o no se cumple el control en su totalidad, la actividad no debería continuar hasta subsanar el hecho (en preventivos), o debería gestionarse la materialización de la causa o riesgo de manera oportuna con acciones correctivas o aclaraciones a las diferencias detectadas.
    - Evidencia: Debe indicar cual es el producto para entregar como evidencia de ejecución del control. Es necesario en la medida de lo posible definir donde reposará las evidencias de ejecución del control.

Ejemplo

Tabla 15: Causas – Control

Causa	Control	Descripción

Inadecuada definición de roles y permisos para el manejo de la página web e intranet por parte del responsable, al momento de la solicitud de asignación de permisos en GLPI a la OIS.	*Verificar los permisos en la intranet y página web mediante solicitud de RQ especificando quienes y que permisos tienen. *Asegurar que los permisos solicitados a la OIS mediante GLPI sean a los profesionales requeridos.	* El profesional asignado o responsable del proceso de Gestión de Comunicaciones, trimestralmente, verifica los permisos en la intranet y página web mediante solicitud de RQ especificando quienes y que permisos tienen. En caso de que se encuentren permisos o roles no permitidos, se solicita la actualización de estos roles por GLPI. Evidencia, solicitud de RQ que reposa en GLPI. * El responsable del proceso de Gestión de Comunicaciones, cada vez que se requiera, asegura que los permisos solicitados a la OIS mediante GLPI sean a los profesionales requeridos, mediante la solicitud de RQ y el diligenciamiento y anexo del Formato establecido. En caso de que se requieran actualizar los permisos o roles asignados, se solicita por GLPI a la OIS. Evidencia, solicitud de RQ que reposa en GLPI.

Fuente: Elaboración propia.

Nota: El control se debe iniciar con un cargo responsable o un sistema o aplicación evitando asignar dependencias y/o áreas de manera general o nombres de personas. El control debe estar asignado a un cargo específico o comité cuando aplique.

Importante: para orientaciones técnicas para valoración de controles, tratamiento (manejo), monitoreo, materialización de riesgos, comunicación y consulta tenga en cuenta lo mencionado en el capítulo 4).

VI. CAPÍTULO 6. RIESGOS AMBIENTALES

Se identifican a partir de la evaluación de aspectos ambientales de acuerdo con el Procedimiento de Identificación de peligros e impactos ambientales (PDT-APO-GFO-006).

VII. CAPÍTULO 7. RIESGOS DE SEGURIDAD Y SALUD EN EL TRABAJO

Se identifican de acuerdo con el diagnóstico que se realice a las instalaciones del FONCEP (FOR-EST-GTH-007).

VIII. CAPÍTULO 8. RIESGOS CONTRACTUALES

El presente capitulo está basado en el “MANUAL PARA LA IDENTIFICACIÓN Y COBERTURA DE RIESGOS EN LOS PROCESOS DE CONTRATACIÓN” expedido por Colombia Compra eficiente-CCE, como máximo ente rector en materia de contratación pública creada mediante Decreto Ley 4170 de 2011.

Para empezar con la exposición del presente capitulo, es menester indicar lo establecido en el artículo 4 de la Ley 1150 de 2007, en el cual se señala lo siguiente:

> *ARTÍCULO 4o. DE LA DISTRIBUCIÓN DE RIESGOS EN LOS CONTRATOS ESTATALES. Los pliegos de condiciones o sus equivalentes deberán incluir la estimación, tipificación y asignación de los riesgos previsibles involucrados en la contratación.*
>
> *En las licitaciones públicas, los pliegos de condiciones de las Entidades estatales deberán señalar el momento en el que, con anterioridad a la presentación de las ofertas, los oferentes y la Entidad revisarán la asignación de riesgos con el fin de establecer su distribución definitiva.*

Dicho lo anterior, el Decreto 1082 de 2015, define el riesgo como: "*Evento que puede generar efectos adversos y de distinta magnitud en el logro de los objetivos del Proceso de Contratación o en la ejecución de un Contrato"*, pero no todo riesgo es considerado un riesgo contractual, por lo que es importante hacer referencia a los riesgos previsibles en materia de contratación.

Así pues, los riesgos previsibles son todos los eventos que puedan afectar la realización de la ejecución contractual y cuya ocurrencia no puede ser predicha de manera exacta por parte de las partes involucradas en el proceso de contratación.

Por lo anterior, la administración de estos riesgos debe cubrir desde la planeación hasta la terminación del plazo, liquidación del contrato, vencimiento de las garantías o la disposición final del bien, obra o servicio.

Ahora bien, teniendo en cuenta las directrices de Colombia Compra Eficiente, el FONCEP, con el ánimo de reducir la exposición de riesgos de los procesos contractuales establece para la definición y valoración de riesgos tener en cuenta los siguientes aspectos:

(a) Los eventos que impidan la adjudicación y firma del contrato como resultado del proceso de contratación.
(b) Los eventos que alteren la ejecución del contrato.
(c) El equilibrio económico del contrato.
(d) La eficacia del proceso de contratación, es decir, que la Entidad Estatal pueda satisfacer la necesidad que motivó el proceso de contratación.
(e) La reputación y legitimidad de la Entidad Estatal encargada de prestar el bien o servicio.

Con esta metodología el FONCEP, busca proporcionar un mayor nivel de certeza y conocimiento para la toma de decisiones relacionadas con el proceso de contratación; mejorar la planeación de contingencias del proceso de contratación; incrementar el grado de confianza entre las partes; y reducir la posibilidad de litigios.

Dicho lo anterior, se presenta el ciclo de gestión de esta tipología de riesgos el cual se define en 5 etapas, así:

1. Establecer el contexto en el cual se adelanta el Proceso de Contratación.
2. Identificar y clasificar los Riesgos del Proceso de Contratación.
3. Evaluar y calificar los Riesgos.
4. Asignar y tratar los Riesgos.
5. Monitorear y revisar la gestión de los Riesgos.

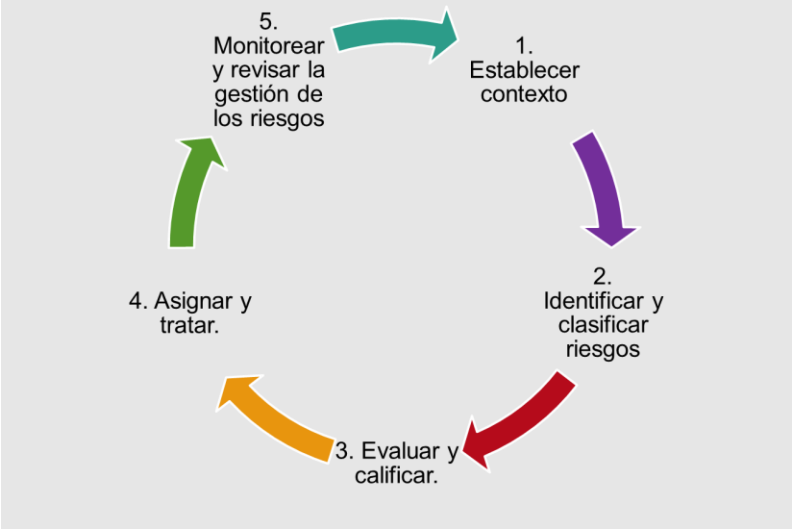

Ilustración 3: Ciclo de gestión del riesgo contractuales

Fuente: Elaboración propia.

Estas etapas deben verse reflejadas en la matriz de identificación de riesgos la cual se encuentra en el aplicativo SVE bajo el "Formato Matriz de Riesgos Transitorios Contractuales FOR-APO-GCN-027" y la cual incluye la clasificación, probabilidad, impacto, la parte que asume el riesgo, los tratamientos y características del monitoreo.

A continuación, se presentan desagregadas las etapas del ciclo de gestión del riesgo así:

1. **Establecer el contexto en el cual se adelanta el Proceso de Contratación.**

En esta etapa el supervisor del contrato debe identificar el contexto con el cual interactúa el FONCEP, y para lo cual debe identificar: objeto del proceso contractual, participes del procesos, ciudadanía que se beneficia de este, disponibilidad de recursos y conocimientos para el proceso de contratación, presupuesto oficial, condiciones geográficas o lugar de ejecución del contrato, entorno socio ambiental, político, factores ambientales, el sector del objeto del proceso, normatividad aplicable, experiencia propia y de otras Entidades en procesos del mismo tipo.

2. Identificar y clasificar los riesgos del proceso de contratación.

Una vez conocido el contexto del proceso contractual, se debe identificar e incluir los riesgos en el "Formato Matriz de Riesgos Transitorios Contractuales FOR-APO-GCN-027". Esta identificación parte del análisis realizado en el contexto, pero también puede ser producto de revisión de riesgos identificados por otras Entidades, lluvia de ideas, análisis DOFA o una encuesta aplicada.

Una vez identificados los riesgos, se debe realizar su clasificación de clase, fuente y etapa de proceso, para lo cual se detalla a continuación la descripción de cada uno de ellos, para una mayor claridad y entendimiento por parte de los estructuradores:

Clase

- **General:** Es un riesgo asociado a todos los procesos de contratación adelantados por la Entidad Estatal, por lo cual está presente en toda su actividad contractual.
- **Específico:** Es un riesgo propio del proceso de contratación objeto de análisis.

Fuente

- **Interno:** Es un riesgo asociado a la operación, capacidad, o situación particular de la Entidad Estatal (ejemplo: reputacional, tecnológico, administrativo, entre otros).
- **Externo:** Es un riesgo del sector del objeto del proceso de contratación, o asociado a asuntos no referidos a la Entidad Estatal (ejemplo: desastres económicos, existencia de monopolios, circunstancias electorales).

Etapa:

La administración de estos riesgos debe cubrir desde la planeación hasta la terminación del plazo, liquidación del contrato, vencimiento de las garantías o la disposición final del bien, obra o servicio. Por lo anterior, **se debe identificar e incluir en la matriz mínimo (un) 1 riesgo por cada etapa del proceso de contratación explicadas a continuación.**

- **Planeación:** La etapa de planeación está comprendida entre la elaboración del Plan Anual de Adquisiciones y la fecha en la cual se decide continuar o no con el proceso de contratación. Durante esta etapa, la Entidad Estatal elabora los estudios previos y el proyecto de pliegos de condiciones o sus equivalentes. Dentro de las preguntas que la Entidad Estatal debe hacerse para identificar los riesgos de la etapa de planeación se encuentran las siguientes:
  - La modalidad de contratación es adecuada para el bien servicio u obra necesitado.
  - Los requisitos habilitantes son los apropiados para el proceso de contratación y es posible encontrar proponentes que los cumplan incluyendo los riesgos relacionados con la habilidad para determinar requisitos habilitantes consistentes con el proceso de contratación y con el sector económico en el que actúan los posibles oferentes.
  - El valor del contrato corresponde a los precios del mercado.
  - La descripción del bien o servicio requerido es clara.
  - El proceso de contratación cuenta con las condiciones que garanticen la transparencia, equidad y competencia entre los proponentes.
  - El estudio de mercado permite identificar los aspectos de oferta y demanda del mercado respectivo.
  - El diseño del proceso de contratación permite satisfacer las necesidades de la Entidad Estatal, cumplir su misión y es coherente con el cumplimiento de sus objetivos y metas.

- **Selección:** La etapa de selección está comprendida entre el acto de Apertura del proceso de contratación y su adjudicación o la declaración de desierto. En la etapa de selección la Entidad Estatal selecciona al contratista. En esta etapa los riesgos frecuentes son los siguientes:
  - Falta de capacidad de la Entidad para promover y adelantar la selección del contratista.
  - Selección de aquellos que no cumplan con la totalidad de los requisitos habilitantes o se encuentren incursos en alguna inhabilidad o incompatibilidad.
  - Riesgo de colusión.
  - Riesgo de ofertas artificialmente bajas

- **Contratación:** Una vez adjudicado el contrato objeto del Proceso de Contratación, inicia la etapa de contratación en la cual se debe cumplir con el cronograma previsto para la celebración del contrato, el registro presupuestal, la publicación en el SECOP y el cumplimiento de los requisitos para el perfeccionamiento, ejecución y pago. En esta etapa los riesgos frecuentes son los siguientes:
  - Riesgo de que no se firme el contrato.
  - Riesgo de que no se presenten las garantías requeridas en los Documentos del Proceso de Contratación o que su presentación sea tardía.
  - Riesgos asociados al incumplimiento de la publicación o el registro presupuestal del contrato.
  - Riesgos asociados a los reclamos de terceros sobre la selección del oferente que retrasen el perfeccionamiento del contrato.

  - **Ejecución:** La etapa de ejecución inicia una vez cumplidos los requisitos previstos para iniciar la ejecución del contrato respectivo y termina con el vencimiento del plazo del contrato o la fecha de liquidación si hay lugar a ella. Esta etapa puede extenderse cuando hay lugar a garantías de calidad, estabilidad y mantenimiento, o a condiciones de disposición final o recuperación ambiental de las obras o bienes. En esta etapa se cumplen con las obligaciones previstas en el contrato, permitiendo el logro del objeto del proceso de contratación; en consecuencia, los riesgos frecuentes son los asociados al cumplimiento del contrato y el logro del objeto propuesto, el rompimiento del equilibrio económico del contrato, los asociados a la liquidación y terminación del contrato y aquellos relacionados con el incumplimiento de la normativa posconsumo.

  Postcontractual: Esta etapa inicia con el vencimiento del plazo de ejecución y finaliza con la liquidación del contrato y acta de cierre de las obligaciones posteriores a la liquidación en los casos previstos en la Ley.

Tipo:

El Documento Conpes 3714 de 2011 clasifica los Riesgos de acuerdo con los siguientes tipos:

- **Riesgos Económicos**: son los derivados del comportamiento del mercado, tales como la fluctuación de los precios de los insumos, desabastecimiento y especulación de estos, entre otros.
- **Riesgos Sociales o Políticos:** son los derivados de los cambios de las políticas gubernamentales y de cambios en las condiciones sociales que tengan impacto en la ejecución del contrato.

- **Riesgos Operacionales:** son los asociados a la operatividad del contrato, tales como la suficiencia del presupuesto oficial, del plazo o los derivados de procesos, procedimientos, parámetros, sistemas de información y tecnológicos, equipos humanos o técnicos inadecuados o insuficientes.
- **Riesgos Financieros:** son (i) el riesgo de consecución de financiación o riesgo de liquidez para obtener recursos para cumplir con el objeto del contrato, y (ii) el riesgo de las condiciones financieras establecidas para la obtención de los recursos, tales como plazos, tasas, garantías, contragarantías, y refinanciaciones, entre otros.
- **Riesgos Regulatorios:** derivados de cambios regulatorios o reglamentarios que afecten la ecuación económica del contrato.
- **Riesgos de la Naturaleza:** son los eventos naturales previsibles en los cuales no hay intervención humana que puedan tener impacto en la ejecución del contrato, por ejemplo, los temblores, inundaciones, lluvias, sequías, entre otros.
- **Riesgos Ambientales:** son los derivados de las obligaciones legales o reglamentarias de carácter ambiental, así como de las licencias, planes de manejo o de permisos y autorizaciones ambientales, incluyendo tasas retributivas y compensatorias, obligaciones de mitigación, tareas de monitoreo y control, entre otras.
- **Riesgos Tecnológicos:** son los derivados de fallas en los sistemas de comunicación de voz y de datos, suspensión de servicios públicos, nuevos desarrollos tecnológicos o estándares que deben ser tenidos en cuenta para la ejecución del contrato, obsolescencia tecnológica. [2]

Una vez identificado lo anterior, se debe realizar una descripción del riesgo, para lo cual se debe describir cada uno de los riesgos de manera clara y específica, para esto tenga en cuenta el catálogo de riesgos creado el cual se encuentra en el formato Excel en la segunda hoja del formato "*Matriz de Riesgos Transitorios Contractuales FOR-APO-GCN-027"*

En la casilla "Consecuencia": Tenga en cuenta que se debe determinar las posibles consecuencias de la ocurrencia de los mismos.

[2] Tomado de https://www.colombiacompra.gov.co/sites/default/files/manuales/cce_manual_riesgo_web.pdf

IDENTIFICACIÓN						
N°	Clase	Fuente	Etapa	Tipo	DESCRIPCIÓN DEL RIESGO (Qué puede pasar y, como puede ocurrir)	CONSECUENCIA (de la ocurrencia del riesgo)
1	General	Externo	Ejecución	Operacionales	Demoras en la presentación y/o entrega de productos o informes por parte del contratista	Incumplimiento de objetivos propuestos

Ilustración 4: Identificación riesgo contractual

Fuente: Elaboración propia.

3. Evaluar y calificar los Riesgos.

En esta etapa se debe evaluar cada uno de los riesgos identificados, estableciendo el impacto de estos frente al logro de los objetivos del proceso de contratación y su probabilidad de ocurrencia.

Esta evaluación tiene como fin asignar a cada riesgo una calificación en términos de impacto y de probabilidad, la cual permite establecer la valoración de los Riesgos identificados y las acciones que se deban efectuar.

Para estimar el impacto y la probabilidad de ocurrencia de un evento que afecte de manera negativa el proceso de contratación, se sugiere considerar fuentes de información como:

- Registros anteriores de la ocurrencia del evento en procesos de contratación propios y de otras Entidades Estatales.

- Experiencia relevante propia y de otras Entidades Estatales.
- Prácticas y experiencia de la industria o el sector en el manejo del riesgo identificado.
- Publicaciones o noticias sobre la ocurrencia del riesgo identificado.
- Opiniones y juicios de especialistas y expertos.
- Estudios técnicos.

La Entidad Estatal debe evaluar los riesgos combinando la probabilidad de ocurrencia y el impacto.

Tabla 16: Escala de probabilidad de riegos contractuales

Probabilidad de Ocurrencia del Riesgo FONCEP					
Nivel	**Escala**	**Descripción**	**Cualitativa**	**Cuantitativa**	**Descripción riesgos transitorios**
1	RARO	Ocurre en circunstancias excepcionales.	No se ha presentado en los últimos 5 años	0-20%	La probabilidad de que el riesgo se materialice es muy baja, solo podría ocurrir en circunstancias excepcionales, fuera del alcance de la Entidad.
2	IMPROBABLE	Puede ocurrir en algún momento. Poco común o frecuente	Se presentó una vez en los últimos 5 años	21-40%	La probabilidad de que el riesgo se materialice es baja, podría ocurrir en circunstancias especiales, dentro del alcance de la Entidad. Existe histórico de que se haya presentado alguna vez en los últimos 5 años en algún contrato ejecutado
3	POSIBLE	Es posible que suceda en algún momento	Se presentó una vez en los últimos 2 años.	41-60%	El riesgo podría materializarse al menos una vez, en etapas previas a la ejecución del plan o del contrato. Existe histórico de que se haya presentado al menos una vez en los últimos 2 años en algún contrato ejecutado

4	PROBABLE	Ocurre en la mayoría de los casos	Se presentó una vez en el último año	61-80%	El riesgo podría materializarse al menos una vez durante la ejecución del plan o del contrato. Existe histórico de que se haya presentado al menos una vez en el último año en algún contrato ejecutado
5	CASI SEGURO	El evento ocurre en la mayoría de las circunstancias. Es muy seguro que se presente.	Se ha presentado más de una vez al año	81-100%	El riesgo podría materializarse más de una vez durante la ejecución del plan o del contrato. Existe histórico de que se haya presentado más de una vez en el último año en algún contrato ejecutado.

Fuente: Elaboración propia.

Tabla 17: Escala de Impacto de riesgos contractuales

Nivel	Escala	cualitativa	cuantitativa
1	Insignificante	Obstruye la ejecución de manera intrascendente	Los sobrecostos no representan más del 1 % del valor del contrato
2	Menor	Dificulta la ejecución de manera baja, aplicando medidas mínimas se puede lograr el objeto	Los sobrecostos representan entre 2% y 5% del valor del contrato
3	Moderado	Afecta la ejecución sin afectar el beneficio para las partes	Los sobrecostos representan entre 5% y 15% del valor del contrato
4	Mayor	Obstruye la ejecución sustancialmente, pero aun así permite el logro del objeto	Los sobrecostos representan entre 16% y 30% del valor del contrato
5	Catastrófico	Perturba la ejecución de manera grave, imposibilitando el logro del objeto	Los sobrecostos representan más del 31 % del valor del contrato

Fuente: Elaboración propia.

Para cada riesgo se deben cruzar las valoraciones de probabilidad e impacto, para obtener la valoración total del riesgo y su categoría. Estas categorías son baja, moderada, alta y extrema, como se muestra a continuación:

Tabla 18: Valoración y categoría de riesgos contractuales

		Impacto				
Probabilidad		1	2	3	4	5
	5	Alta	Alta	Extrema	Extrema	Extrema
	4	Moderada	Alta	Alta	Extrema	Extrema
	3	Baja	Moderada	Alta	Extrema	Extrema
	2	Baja	Baja	Moderada	Alta	Extrema
	1	Baja	Baja	Moderada	Alta	Extrema

Fuente: Elaboración propia.

Lo anterior, se puede evidenciar en el formato "*Matriz de Riesgos Transitorios Contractuales FOR-APO-GCN-027",* de la siguiente forma:

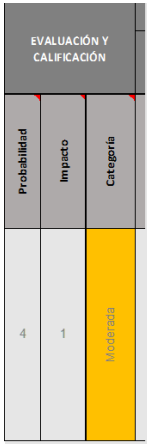

Ilustración 5: Evaluación y calificación de riesgos contractuales

Fuente: Elaboración propia.

4. Asignar y tratar los Riesgos.

Una vez realizada la evaluación y calificación de cada uno de los riesgos asociados al proceso de contratación, se debe establecer un orden a cada una de las siguientes opciones de tratamiento:

- **Evitar el Riesgo**: para lo cual debe decidir no proceder con la actividad que causa el riesgo o buscar alternativas para obtener el beneficio del Proceso de Contratación.
- **Transferir el Riesgo**: haciendo responsable a otra Entidad quien asume las consecuencias de la materialización del riesgo, típicamente se transfiere el riesgo a través de las garantías previstas en el proceso de contratación o en las condiciones del contrato estableciendo con claridad quien es el responsable. El principio general es que el riesgo debe asumirlo la parte que pueda enfrentarlo en mejor forma, bien sea por su experiencia, conocimiento o papel dentro de la ecuación contractual, entre otras.
- **Aceptar el Riesgo**: cuando no puede ser evitado ni ser transferido o el costo de evitarlo o transferirlo es muy alto. En este caso se recomiendan medidas para reducir el riesgo o mitigar su impacto, así como el monitoreo.
- **Reducir la probabilidad de la ocurrencia del evento**: cuando el Riesgo debe ser aceptado. Para el efecto se sugieren medidas como: (i) aclarar los requisitos, requerimientos y especificaciones y productos del contrato; (ii) revisar procesos; (iii) establecer sistemas de aseguramiento de calidad en los contratos; (iv) especificar estándares de los bienes y servicios; (v) hacer pruebas e inspecciones de los bienes; (vi) establecer sistemas de acreditación profesional; (vii) incluir declaraciones y garantías del contratista; (viii) administrar la relación entre proveedores y compradores.
- **Reducir las consecuencias o el impacto del Riesgo**: a través de planes de contingencia, en los términos y condiciones del contrato, inspecciones y revisiones para revisar el cumplimiento del contrato y programas de apremio para lograr el cumplimiento del contrato.

Estas acciones deben seleccionarse teniendo en cuenta el costos y beneficio del riesgo. Se puede combinar las opciones de tratamiento para un mejor resultado. Generalmente estas medidas son acciones específicas para responder a los eventos; para lo cual se sugiere preparar un plan de tratamiento para documentar como se enfrenta cada uno de los riesgos incluyendo acciones, cronogramas, recursos (personal, información) y presupuesto, responsabilidades, necesidades de informes y reportes y de monitoreo. Tenga en cuenta para asignar el riesgo, se debe considerar quien es el agente generador.

La tarea más importante del manejo del riesgo es la implementación del plan de tratamiento, lo cual requiere atención, asegurar los recursos que requiere y el cumplimiento oportuno de las tareas previstas en este plan. La matriz debe contener la información básica del tratamiento de los Riesgos.

Lo anterior debe verse contemplado en la siguiente parte del formato "*Matriz de Riesgos Transitorios Contractuales FOR-APO-GCN-027*":

TRATAMIENTO								
Opción de Manejo					Tratamiento Proyectado		PLAZO ESTIMADO (Tratamiento)	
Evitar	Compartir o Transferir	Asumir	Reducir Probabilidad	Reducir Impacto	Tratamiento específico / Controles a realizar	Responsable del tratamiento	Etapa Inicio	Etapa Fin
X					El supervisor de contrato realizará seguimiento al cumplimiento de las obligaciones contractuales, a través de la verificación de los informes mensuales de ejecución y entregables presentados por el contratista. En caso de evidenciar incumplimiento de las obligaciones, el supervisor requerirá por escrito al contratista, con el fin de adelantar las acciones de mejora correspondientes.	Supervisor	Etapa Postcontractual	Etapa Postcontractual

Ilustración 6: Tratamiento de riesgos contractuales

Fuente: Elaboración propia.

5. Monitorear y revisar la gestión de los Riesgos.

Los riesgos identificados deben monitorearse constantemente por parte de los supervisores. Para esto, es importante mencionar que los riesgos cambian rápidamente pues no son estáticos. Por tal razón se debe revisar los riesgos permanentemente, de acuerdo con la periodicidad de seguimiento establecida en el formato y revisar si es necesario hacer ajustes en el plan de tratamiento.

El fin del monitoreo es:

- Garantizar que los controles son eficaces y eficientes en el diseño y en la operación.

- Obtener información adicional para mejorar la valoración del riesgo.
- Analizar y aprender lecciones a partir de los eventos, los cambios, las tendencias, los éxitos y los fracasos.
- Detectar cambios en el contexto externo e interno que puedan exigir revisión de los tratamientos del riesgo y establecer un orden de prioridades de acciones para el tratamiento del Riesgo.
- Identificar nuevos riesgos que pueden surgir.

Metodología del monitoreo

- El monitoreo de los riesgos se realizará mediante un muestreo el cual se realizará con los siguientes parámetros:

  1. La selección de contratos por modalidad de contratación (Mínima cuantía, licitación pública, concurso de méritos, selección abreviada y contratación directa).
  2. La selección teniendo en cuenta el que tenga la mayor cantidad de recursos y aquel que no se le haya hecho seguimiento en periodos anteriores, de por lo menos un contrato de prestación de servicios por supervisor en cada trimestre.

- Para el monitoreo se tendrá en cuenta las etapas (Planeación, selección, contratación y ejecución) y el trimestre del año sobre el cual se esté realizando el seguimiento. Por ejemplo, si se realiza durante el primer y segundo trimestre del año, el monitoreo se puede realizar sobre las etapas de planeación, selección y contratación. En el caso que se haga en el último trimestre de la vigencia, el monitoreo se hará a la etapa de ejecución, dependiendo de la fecha de adjudicación del contrato.
- El monitoreo se realizará mediante un archivo en Excel dispuesto en ONEDRIVE, en el cual cada dependencia tendrá acceso para realizar el seguimiento correspondiente según la muestra seleccionada y el cargue de las evidencias en los periodos de tiempos establecidos para el seguimiento por la Oficina Asesora Jurídica.
- La Oficina Asesora Jurídica elaborará como segunda línea de defensa el informe sobre monitoreo a los riesgos transitorios contractuales, por lo cual se solicitará el seguimiento a los supervisores de manera trimestral mediante correo electrónico.

Lo anterior, debe incluirse en la siguiente parte del formato:

FORMA DE MONITOREO PLANEADA		MONITOREO PRIMER TRIMESTRE							EVALUACION FINAL REAL (solo si se materializa el riesgo)		
Cómo se realizará el monitoreo?	Periodicidad. Cuándo?	Fecha Monitoreo	¿Se Materializó el Riesgo?	Si su respuesta fue si en la columna AB, indique ¿Qué sucedió y cual fue su impacto?	¿Se ejecutaron las actividades de control o tratamiento como fueron diseñadas?	¿Cual es la evidencia y donde reposan?	¿Se debe modificar, mantener o crear nuevas acciones de tratamiento o controles ?	Si su respuesta fue si en las columnas AB, AD y se crean o modifican las acciones en la columna AF, por favor indique las acciones.	Probabilidad	Impacto	Categoría
Revisión mensual de los informes de ejecución del contrato y entregables. La evidencia de este control es el informe mensual de supervisión del contrato.	Mensual	30/03/2021	Si	Se materializó el riesgo, se notifico mediante correo electronico con fecha del 15 /03/2021 a la OAJ , se formularon acciones nuevas de control.	Si	Correo electronico remitido por el supervisor del contrao y hace parte del expediente contractual	Crear	Se crean los siguientes acciones: Registro documental de las actividades	3	3	Alta

Ilustración 7: Monitoreo de riesgos contractuales

Fuente: Elaboración propia.

Es responsabilidad del supervisor realizar el monitoreo tanto en la matriz de riesgos y en el formato Informe de supervisión establecido en el proceso de gestión contractual.

En caso de que se materialice un riesgo, los supervisores deben:

- Notificar a la segunda línea de defensa (Oficina Asesora Jurídica) mediante correo electrónico cada vez que se materialice un riesgo.
- Definir los controles o acciones de tratamientos nuevos que ataquen la causa de la materialización del riesgo.
- Reportar esta información en el siguiente monitoreo de riesgos transitorios contractuales.
- Actualizar la probabilidad e impacto en el último monitoreo de la vigencia.

Con el fin de actualizar los controles o acciones de tratamiento nuevos, posterior al reporte de la materialización del riesgo el supervisor debe:

1. En el formato del INFORME DE SUPERVISIÓN FOR-APO-GCN-030, en el numeral No 7 Análisis materialización y mitigación del riesgo en las observaciones, relacionar la materialización del riesgo y a su vez indicar las acciones de tratamiento nuevo y/o actualizaciones realizadas a la matriz de riesgo transitorios contractuales especificando los cambios realizados.
2. Identificar la necesidad de modificar la matriz de riesgos del contrato, especificando los cambios a realizar.
3. Anexar al Informe de supervisión la **Matriz de Riesgos Transitorios Contractuales FOR-APO-GCN-027** actualizada
4. Enviar la matriz de riesgo ajustada a la Oficina Asesora Jurídica con el fin de actualizar la base del monitoreo de riesgos contractuales.

Finalmente es importante señalar que los riesgos cubiertos bajo el Régimen de Garantías[3], esto es que pueden mitigarse o hacerse efectivos, a través de los amparos constituidos en las garantías del proceso y que son lo que se derivan del cumplimiento de las obligaciones contractuales, no son sujeto de ser plasmados en el formato de matriz de riesgos.

A manera de ejemplo no se consideran riesgos transitorios:

- El incumplimiento total o parcial del contrato
- Los hechos derivados de la responsabilidad extracontractual
- Los que corresponden a la teoría de la imprevisión (Temblores, terremotos, incendios…)
- Las inhabilidades e incompatibilidades sobrevinientes (Cesión de contrato)

IX. CAPITULO 9. RIESGOS FIDUCIARIOS

Los riesgos fiduciarios deben concebirse como derivados de los riesgos financieros, por lo cual, se hace necesaria la consulta a las definiciones otorgadas por el ente supervisor de las sociedades fiduciarias, como lo es, la Superintendencia Financiera de Colombia (En adelante, SFC) en cuanto al Marco Integral de Supervisión definido por la misma.

Es de mencionar que este marco se adopta teniendo en cuenta el tamaño y los negocios que realicen entre el FONCEP y las sociedades fiduciarias, en el entendido que se podrán evidenciar algunas instrucciones expedidas por la SFC que no aplican a las actividades que se llevan dentro esta relación

[3] Garantías tales como: seriedad de la oferta, cumplimiento del contrato, calidad de los bienes y servicios, estabilidad de la obra, salarios y prestaciones sociales, buen manejo del anticipo, responsabilidad civil extracontractual

contractual. De esta manera, el FONCEP establece que en la identificación de estos riesgos deben basarse bajo la tipología especifica de riesgos que se definen a continuación:

Tabla 19: Definición tipología de riesgos para la identificación de riesgos fiduciarios

Tipo de Riesgo	Definición
Riesgo de crédito y/o contraparte	Se entiende como la posible pérdida o disminución de los activos financieros como consecuencia de que la contraparte incumpla sus obligaciones.
Riesgo de mercado	Son las variaciones en el valor del portafolio por efectos de cambios en el precio y/o tasas de interés, de los activos que componen los portafolios de inversión.
Riesgo de liquidez	El riesgo de liquidez se define como la incapacidad para cumplir plenamente, de manera oportuna y eficiente los flujos de caja esperados, vigentes y futuros de los patrimonios autónomos, de acuerdo con las necesidades proyectadas.
Riesgo operativo	Se entiende por riesgo operativo la posibilidad de incurrir en pérdidas por las deficiencias, fallas o inadecuado funcionamiento de los procesos, la tecnología, la infraestructura o el recurso humano, así como por la ocurrencia de acontecimientos externos asociados a éstos.
Riesgo de lavado de activos	Es la posibilidad de pérdida o daño por su propensión a ser utilizada, directamente o través de sus operaciones, como instrumento para la canalización de recursos hacia la realización de actividades terroristas o cuando se pretende el ocultamiento de activos provenientes de dichas actividades.
Riesgo de cumplimiento – legal	El riesgo de cumplimiento está definido como la pérdida económica potencial por el incumplimiento de normas o disposiciones legales, por lo que la Fiduciaria debe asegurarse de entender las disposiciones legales de la operación del negocio; este riesgo también incluye el riesgo legal como consecuencia de fallas en los contratos o la imposibilidad legal de ejecutar un contrato debido a fallas en la implementación legal.

Fuente: Elaboración propia a partir de la información de la Superintendencia Financiera de Colombia.

Una vez se cuenta con la tipología de los riesgos, la gestión de riesgos fiduciarios debe estar orientada en la identificación temprana de los mismos en las etapas que se describen a continuación:

- **Etapa precontractual:** Hace referencia al periodo en el cual se adelanta el proceso de contratación con la fiduciaria y los esfuerzos en la identificación de riesgos deben enfocarse en el contexto con el cual interactúa FONCEP con esta Entidad financiera mientras se están llevando a cabo los respectivos procesos de licitación hasta la suscripción del contrato.

- **Etapa contractual:** En esta etapa se consideran los procesos que se llevan a cabo durante la ejecución del contrato con la fiduciaria. Por lo cual, el enfoque de la gestión de riesgos debe realizarse en el seguimiento de los procesos que se llevan a cabo con la Entidad financiera y las posibles desviaciones respecto a las condiciones contractuales pactadas.
- **Etapa post-contractual:** La etapa post-contractual hace referencia a la finalización del contrato por vencimiento de términos o de manera anticipada por diferentes eventos. Es así como, el enfoque de la gestión de riesgos en esta etapa debe hacerse orientada en los procesos de liquidación financiera y finalización de obligaciones contractuales, con el fin de llevar a feliz término la relación contractual entre FONCEP y la sociedad fiduciaria.

Identificación de Riesgos

La tipología de riesgos y las etapas mencionadas anteriormente brindan una herramienta para la identificación de los riesgos fiduciarios basado en las orientaciones mencionadas en la siguiente tabla:

Tabla 20: Tipología de riesgos y etapas contractuales con la sociedad fiduciaria.

Tipo de Riesgo	Etapa Pre-Contractual	Etapa Contractual	Etapa Post-Contractual
Riesgo de crédito y/o contraparte	Deben considerarse los distintos escenarios donde la fiduciaria podría incurrir en el incumplimiento de sus obligaciones con FONCEP e incluir mecanismos de cobertura frente a posibles materializaciones del riesgo en las condiciones del contrato, previo a su suscripción.	Deben considerarse las señales de alerta que indiquen posibles incumplimientos de las obligaciones de la fiduciaria con FONCEP, tales como: Cambios en calificación crediticia, deterioro en los estados financieros, deterioro de los portafolios de inversión, entre otros.	Deben considerarse los posibles incumplimientos de las obligaciones de la fiduciaria con FONCEP, al momento de la liquidación del contrato. Por lo cual, se hace necesaria la definición de los planes de contingencia y la medición de los impactos financieros ante las posibles materializaciones de los riesgos
Riesgo de mercado	Deben considerarse los distintos escenarios donde la fiduciaria podría incurrir en el deterioro del portafolio de inversión por cambios en el precio y/o tasas de interés, de los activos que componen el mismo e incluir mecanismos de cobertura frente a posibles materializaciones del	Deben considerarse las señales de alerta que indiquen posibles deterioros en el valor del portafolio de inversión por cambios en el precio y/o tasas de interés, de los activos que componen el mismo, apoyado en	Deben considerarse las posibles variaciones negativas en el valor del portafolio de inversión por cambios en el precio y/o tasas de interés, de los activos que componen el mismo, al momento de la liquidación del contrato. Por lo cual, se hace

Tipo de Riesgo	Etapa Pre-Contractual	Etapa Contractual	Etapa Post-Contractual
	riesgo en las condiciones del contrato, previo a su suscripción.	el seguimiento constante de los mercados financieros.	necesaria la definición de los planes de contingencia y la medición de los impactos financieros ante las posibles materializaciones de los riesgos.
Riesgo de liquidez	Deben considerarse los distintos escenarios donde la fiduciaria podría incurrir en el incumplimiento de los flujos de caja esperados, vigentes y futuros con FONCEP e incluir mecanismos de cobertura frente a posibles materializaciones del riesgo en las condiciones del contrato, previo a su suscripción.	Deben considerarse las señales de alerta que indiquen posibles incumplimientos de los flujos de caja esperados, vigentes y futuros de la fiduciaria con FONCEP, tales como: Cambios en calificación crediticia, deterioro en los estados financieros, deterioro de los portafolios de inversión, entre otros.	Deben considerarse los posibles incumplimientos de los flujos de caja esperados, vigentes y futuros con FONCEP, al momento de la liquidación del contrato. Por lo cual, se hace necesaria la definición de los planes de contingencia y la medición de los impactos financieros ante las posibles materializaciones de los riesgos
Riesgo operativo	Deben considerarse los distintos escenarios donde FONCEP incurra en pérdidas por las deficiencias, fallas o inadecuado funcionamiento de los procesos, la tecnología, la infraestructura o el recurso humano de la fiduciaria, así como por la ocurrencia de acontecimientos externos asociados a esta, e incluir mecanismos de cobertura frente a posibles materializaciones del riesgo en las condiciones del contrato, previo a su suscripción.	Deben considerarse las señales de alerta que indiquen posibles pérdidas a FONCEP por las deficiencias, fallas o inadecuado funcionamiento de los procesos, la tecnología, la infraestructura o el recurso humano de la fiduciaria, así como por la ocurrencia de acontecimientos externos asociados a ésta, tales como: Funcionarios no idóneos, tecnología poco apropiada, deficiencias en los procesos, entre otros.	Deben considerarse los posibles incumplimientos por las deficiencias, fallas o inadecuado funcionamiento de los procesos, la tecnología, la infraestructura o el recurso humano de la fiduciaria, así como por la ocurrencia de acontecimientos externos asociados a ésta con FONCEP, al momento de la liquidación del contrato. Por lo cual, se hace necesaria la definición de los planes de contingencia y la medición de los impactos financieros ante las posibles materializaciones de los riesgos
Riesgo de lavado de activos	Deben considerarse los distintos escenarios donde la fiduciaria podría incurrir en la	Deben considerarse las señales de alerta que indiquen posibles	Deben considerarse los posibles hallazgos de canalizaciones de

Tipo de Riesgo	Etapa Pre-Contractual	Etapa Contractual	Etapa Post-Contractual
	canalización de recursos hacia la realización de actividades terroristas o el ocultamiento de activos provenientes de dichas actividades, haciendo uso de los patrimonios autónomos con FONCEP e incluir mecanismos de cobertura frente a posibles materializaciones del riesgo en las condiciones del contrato, previo a su suscripción.	canalizaciones de recursos hacia la realización de actividades terroristas u ocultamientos de activos provenientes de dichas actividades, haciendo uso de los patrimonios autónomos con FONCEP, tales como transacciones u operaciones atípicas, relación de la fiduciaria con agentes relacionados en listas restrictivas, entre otros.	recursos hacia la realización de actividades terroristas u ocultamientos de activos provenientes de dichas actividades, al momento de la liquidación del contrato. Por lo cual, se hace necesaria la definición de los planes de contingencia y la medición de los impactos reputacionales, legales, ante las posibles materializaciones de los riesgos
Riesgo de cumplimiento – legal	Deben considerarse los distintos escenarios donde la fiduciaria podría incurrir en el incumplimiento de normas o disposiciones legales con FONCEP e incluir mecanismos de cobertura frente a posibles materializaciones del riesgo en las condiciones del contrato, previo a su suscripción.	Deben considerarse los distintos escenarios donde la fiduciaria podría incurrir en el incumplimiento de normas o disposiciones legales con FONCEP, tales como: Actualizaciones de norma, interpretación de normas en beneficio propio, entre otros.	Deben considerarse los posibles incumplimientos de normas o disposiciones legales con FONCEP, al momento de la liquidación del contrato. Por lo cual, se hace necesaria la definición de los planes de contingencia y la medición de los impactos legales y financieros ante las posibles materializaciones de los riesgos

Fuente: Elaboración propia.

Causas y Consecuencias (efectos)

Al identificar los riesgos se indaga sobre sus causas, partiendo del análisis sobre el evento que puede generar el riesgo, el momento que pueda suceder y el agente o factor generador, atendiendo las contrapartes como FONCEP o la fiduciaria.

De otra parte, se deben considerar los efectos por la materialización del riesgo, en este caso, los impactos que afectarían a FONCEP por estos eventos.

Identificación de Controles

Finalmente, los controles se construyen a partir de las causas, y se debe tener en cuenta la definición de los siguientes componentes con el fin de lograr un mejor monitoreo: Responsable de llevar a cabo el control, periodicidad de ejecución, objetivo del control, cómo se realiza la actividad del control, definición de desviaciones en caso de que no se lleve a cabo el control y evidencia del control.

Es de mencionar que, las apreciaciones establecidas en el **Capítulo 4. Riesgos de metas y resultados, de corrupción y de proceso** amplían las instrucciones para la construcción de las **Causas, Consecuencias y los Controles.**

Ejemplo

Luego de haber identificado la tipología del riesgo, la etapa contractual con la fiduciaria y haber definido las causas con sus respectivos controles, el riesgo fiduciario se reflejaría de la siguiente manera.

Tabla 21: Ejemplo riesgo fiduciario

Etapa	Descripción del Riesgo	Causas	Controles/ Acción
Pre-Contractual	Selección de una fiduciaria que no cumpla los requisitos de la licitación o con poca experiencia.	• Definición de requisitos habilitantes bajos o débiles por parte de las áreas que intervienen en el proceso del contrato durante su etapa de planeación. • Inadecuada planeación de los tiempos para contratar la fiducia por parte de las áreas que intervienen en el proceso del contrato en la etapa contractual.	**Control:** Formular la licitación y su cronograma en compañía de las áreas que intervienen en el proceso y dejar la constancia en actas o bitácoras, **Responsable:** por parte del, Profesional especializado de tesorería y profesional asignado de OAJ, **Periodicidad:** cada vez que se formule el estudio previo de la fiducia. **Objetivo:** Asegura la definición de requisitos habilitantes y la planeación de tiempos adecuados, **Como se realiza:** Mediante mesas de trabajo con las áreas que intervienen en el proceso contractual (OAP; OAJ, SFA, entre otros) en donde se definan dichos requisitos y un cronograma de actividades y tiempos máximos para realizar la contratación de la fiducia. **Desviación u Observación:** En caso de no tener asistencia de todas las áreas se realizará la mesa de trabajo con las áreas de cada uno de los enfoques técnicos que asistan, adelantando su aporte a los requisitos y al cronograma. **La evidencia** son las bitácoras y/o actas de las mesas de trabajo.

Aplicativo SVE

Los riesgos fiduciarios serán gestionados a través del aplicativo SVE, siguiendo las apreciaciones establecidas en el **Capítulo 11. Uso módulo riesgos en el aplicativo SVE..** En este sentido, la Subdirección Financiera y Administrativa y el Comité Fiduciario son los actores principales para la implementación y monitoreo de estos riesgos por lo cual podrán apoyarse en el mencionado aplicativo.

X. CAPITULO 10. RIESGO DE LAVADO DE ACTIVOS (LA) Y FINANCIACIÓN DEL TERRORISMO (FT)

Esta clase de riesgo está relacionado con la posibilidad de pérdida o daño que puede sufrir el FONCEP por su propensión a ser utilizada directamente o a través de sus operaciones utilizando los canales ofrecidos, como instrumento para el lavado de activos y/o canalización de recursos hacia la realización de actividades terroristas, o cuando se pretenda el ocultamiento de activos provenientes de dichas actividades.

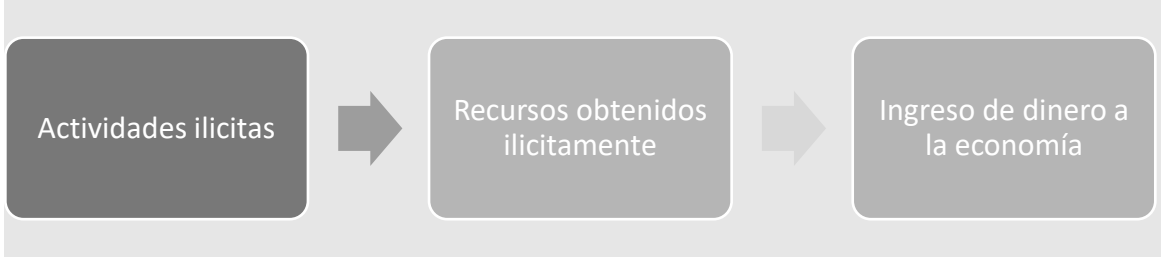

Ilustración 8: Actividades que promueven el LA/FT

Fuente: Elaboración propia.

Si bien FONCEP no genera ingresos derivados de su función social, puede recibir recursos de Entidades privadas, donaciones o inversión externa que puedan estar destinadas a la financiación de proyectos que requieren procesos de contratación los cuales por su número y cuantía son significativos y pueden presentar vulnerabilidad al riesgo de LA/FT. Así mismo, teniendo en cuenta los lineamientos de la Circular 092 de 2020 de la Secretaria General de la Alcaldía Mayor de Bogotá, específicamente la autoevaluación de riesgos operativos SARLAFT, en el cual las respuestas positivas al cuestionario fueron tres (3), lo cual permite entender que el FONCEP tiene un nivel de riesgo operativo “Bajo” según la siguiente gráfica:

- ¿Los clientes objetivo de la Entidad son personas naturales entre las que se encuentran las personas expuestas políticamente (PEP’s)?
- ¿En la Entidad existe una alta rotación de sus proveedores nacionales y extranjeros o los están cambiando con frecuencia?

- ¿La Entidad emplea terceros para llevar a cabo alguna de las funciones en el cumplimiento de sus objetivos?

Nivel de riesgo operativo	*Si el número de respuestas positivas se encuentra entre*
BAJO	1 y 3
MODERADO	4 y 5
MEDIO	6 y 7
ALTO	8 y 9
CRÍTICO	10 y 11

Ilustración 9: Nivel de riesgo operativo - LA/FT

Fuente: Tomado de Circular No.092 de 2020, Secretaria General de la Alcaldía Mayor de Bogotá

De esta manera, para la gestión de riesgo, es necesario contar con las siguientes herramientas:

- Señales de alerta de LA/FT
- Delitos Fuentes de LA/FT
- Etapas de riesgo de LA/FT
- Listas Restrictivas o vinculantes
- Personas Públicamente Expuestas (PEP's)
- Operaciones sospechosas
- Estructura Organizacional
- El funcionario responsable de sistema SARLAFT

Señales de alerta de LA/FT

Las señales de alerta LA/FT son una herramienta importante para la gestión del riesgo LA/FT y hace referencia a las actividades o situaciones que se ven relacionados con los factores internos o externos generadores de este riesgo que afectan la multiplicidad de acciones que realiza FONCEP (Los factores de riesgo pueden ser: los clientes, usuarios, proveedores, empleados, productos, canales de distribución y zonas o jurisdicciones de alto riesgo)

Por lo tanto, cada factor o fuente de riesgo debe contar con sus respectivas señales de alerta, a manera enunciativa, se han definido las siguientes señales de alerta por cada factor:

Factor Cliente: Información insuficiente o falsa entregada por el cliente (agente generador del riesgo).
Factor Empleados: Empleados con un estilo de vida que no corresponde con el monto de su salario.
Factor Productos: Operaciones que por su monto y número no coinciden con la capacidad económica y perfil del cliente.
Factor Proveedores: Proveedores que ofrecen productos a menor precio de los que existen en el mercado; o, inconsistencias en los datos de la empresa, representante legal y/o socios en el proceso de verificación por parte de la Entidad.

Delitos Fuentes de LA/FT

Es de anotar que este riesgo generalmente señala al narcotráfico como principal delito de LA/FT, sin embargo, la Ley 599 de 2000 (Código Penal Colombiano) contempla otras actuaciones prohibidas generadoras de recursos ilícitos. Entre los delitos que se encuentran en la mencionada Ley, se relacionan los siguientes donde se ha identificado cierta vulnerabilidad para FONCEP:

- Enriquecimiento ilícito de particulares (Art. 327).
- Delitos contra el sistema financiero (del Art. 314 al 317), como: Utilización indebida de fondos captados del público; operaciones no autorizadas con accionistas o asociados; captación masiva y habitual de dineros; y, manipulación fraudulenta de especies inscritas en el registro nacional de valores e intermediarios.
- Favorecimiento por servidor público (Art. 322).
- Delitos contra la administración pública (del Art.397 al 434B), como: peculado por apropiación, peculado por uso, peculado por aplicación oficial diferente, entre otros.

Etapas de riesgo de LA/FT

Entre las etapas para el riesgo de LA/FT se encuentran las siguientes según el modelo GAFI[4]:

- **Colocación:** Consiste en la recepción física de bienes de cualquier naturaleza o de dinero, en desarrollo y como consecuencia de actividades ilícitas que pretenden ser puestas en el sistema económico.
- **Transformación:** Consiste en la introducción de los fondos (dinero físico) o bienes, en la economía legal, seguida de sucesivas operaciones (nacionales o internacionales), para ocultar, invertir, o para mezclarlos con dinero de origen legal.
- **Integración:** En este paso, el dinero lavado regresa a la economía en apariencia o como "dinero legítimo".

De acuerdo con lo anterior, en FONCEP se ha identificado el ingreso de recursos públicos para la administración de pensiones y cesantías inicialmente, reduciendo significativamente la materialización de riesgo LA/FT. No obstante, es importante guiarse por las etapas de la administración de riesgo para los procesos que se lleven actualmente en la Entidad, enfocando la atención en el lavado de activos y financiación del terrorismo. Las orientaciones para la administración de riesgo están establecidas en el **Capítulo 3. Etapas de la administración del riesgo,** donde se encuentran: **(i)** las instrucciones para la identificación de riesgos, causas o fallas que pueden dar origen a la materialización del riesgo, identifican el riesgo inicial o inherente; **(ii)** la identificación del control o controles; y, **(iii)** la evaluación de los controles si están bien diseñados para mitigar el riesgo.

Listas restrictivas o vinculantes

Las listas restrictivas o vinculantes relacionan a las personas naturales y jurídicas, que pueden estar vinculadas con actividades de LA/FT. Por lo tanto, estas listas se convierten en una herramienta efectiva en el proceso inicial de conocimiento de los clientes, usuarios, proveedores y empleados, dentro de las cuales se destacan los siguientes:

[4] El Grupo de Acción Financiera Internacional (GAFI) es un organismo intergubernamental independiente que desarrolla y promueve políticas para proteger el sistema financiero mundial contra el lavado de dinero, el financiamiento del terrorismo y la financiación de la proliferación de armas de destrucción masiva. Las Recomendaciones del GAFI son reconocidas como la norma global contra el lavado de dinero (ALD) y contra el financiamiento del terrorismo (CFT) (GAFI (2018), Guía sobre el combate al financiamiento de la proliferación: aplicación de disposiciones financieras de las resoluciones del Consejo de Seguridad de las Naciones Unidas para contrarrestar la proliferación de armas de destrucción masiva, GAFI, París www.fatf-gafi.org/publications/fatfrecommendations/documents/guidancecounter-proliferation-financing.html, pag.2)

Tabla 22: Listas restrictivas o vinculantes

Organismo	Enlace
Consejo de Seguridad de la ONU	https://scsanctions.un.org/r-sp/?keywords=car
Lista OFAC - office of (Foreign Assets Control)	https://sanctionssearch.ofac.treas.gov/
Lista de Terroristas (Foreign Terrorist Organizations)	https://www.state.gov/foreign-terrorist-organizations/ https://www.consilium.europa.eu/es/policies/fight-against-terrorism/terrorist-list/ https://eur-lex.europa.eu/legal-content/es/TXT/HTML/?uri=CELEX:32019D1341&from=en
Consejo de la Unión Europea	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009E0468&qid=1412596355797&from=EN
Interpol	https://www.interpol.int/How-we-work/Notices/View-Red-Notices

Fuente: Elaboración propia.

De esta manera, FONCEP no podrá ejercer actividades económicas o vincular personas naturales o jurídicas que cuenten con coincidencias en las listas anteriormente mencionadas, así mismo, en caso de tener una vinculación actual con alguna persona y que, posteriormente se encuentre relacionada en estas listas, deberá reportarlo a la UIAF y terminar su vinculación inmediatamente, generando una investigación de las transacciones o negocios que haya realizado al interior de la organización.

Personas Públicamente Expuestas (PEP's)

Las Personas Públicamente Expuestas (PEP's) por su perfil o por las funciones que desempeñan exponen en mayor grado a FONCEP al riesgo de LA/FT, por manejar recursos públicos o porque tienen algún grado de poder o de reconocimiento. Por lo cual, se someterán a procedimientos más exigentes y a la creación de mecanismos que permitan identificar las personas que responden a estos perfiles, a manera enunciativa, estas personas deberán declarar: **(i)** Los nombres e identificación de las personas con las que tengan sociedad conyugal, de hecho, o de derecho; **(ii)** los nombres e identificación de sus familiares hasta segundo grado de consanguinidad, primero afinidad y primero civil; y, **(iii)** la existencia de cuentas financieras en algún país extranjero, en caso de que tengan derecho o poder de firma o de otra índole sobre alguna de ellas

Adicionalmente, se contará el registro de clientes, usuarios, Personas Públicamente Expuestas (PEP's), proveedores y la existencia de cambios atípicos en las operaciones como las zonas, los montos y el número de transacciones relacionadas con los productos, bienes o servicios ofrecidos por FONCEP para detectar las operaciones inusuales. Una vez, se confirman estas operaciones se tendrán que remitir a la UIAF de manera oportuna.

En este sentido, la UIAF pone a disposición el Sistema de Reporte en Línea (SIREL) que es un sistema en ambiente web desarrollado como una herramienta para la recepción de los reportes subjetivos como el ROS y de los reportes objetivos de las Entidades de los diferentes sectores, los cuales se cargan en línea de manera eficiente y segura. Es de mencionar que, las operaciones detectadas como sospechosas deben estar soportadas por documentos que permitan evidenciar los cambios significativos de comportamientos asociados con las señales de alerta.

La Oficina Asesora Jurídica es quien coordina la actividad contractual con terceros para suplir la necesidad de bienes, obras o servicios en el FONCEP.

Estructura Organizacional

Serán funciones mínimas a cargo de los órganos de dirección, control y administración los siguientes:

- **Alta dirección:** Hacer seguimiento y pronunciarse periódicamente sobre el perfil de riesgo de LA/FT de la Entidad.
- **Oficina Asesora Jurídica (responsable SARLAFT):** Coordinar la aplicación de los lineamientos de SARLAFT **i)** Velar por el cumplimiento y funcionamiento de las etapas que conforman el SARLAFT de forma efectiva, eficiente y oportuna; y, **(ii)** Acompañar y apoyar transversalmente a las diferentes áreas de FONCEP en el diseño de las metodologías, modelos e indicadores cualitativos y/o cuantitativos de reconocido valor técnico para la oportuna detección de las operaciones inusuales.
- **Supervisores de contrato:** Ejecución de controles del riesgo.

Funciones específicas de responsable SARLAFT

Adelantar la vigilancia de manera permanente (segunda línea de defensa) que permita la detección oportuna de los riesgos de LA/FT. La persona designada para adelantar estas acciones deberá determinar:

- Si los controles aplicados son oportunos y efectivos.
- El seguimiento de los niveles del riesgo inherente y residual de cada factor de riesgo y los riesgos asociados, para establecer su aceptabilidad.
- El seguimiento a las listas vinculantes y otras fuentes del sector, para el monitoreo de las contrapartes donde puede estar relacionado un tercero vinculado.
- Identificar cambios mediante nuevas señales de alerta.

- Determinar fallas en el funcionamiento del sistema SARLAFT.
- Solicitar la actualización de la información de los clientes y/o usuarios, mínimo cada año.
- Implementar documentación que permitan mejorar su gestión como formatos de declaración de fondos o proponer mejoras a los formatos de vinculación a FONCEP, entre otros.
- Realizar capacitaciones de tal manera que se garantice la aplicación de los procedimientos que integran del SARLAFT.
- Reportar la información requerida a las autoridades competentes, entre ellos, el Reporte Operaciones Sospechosas (ROS) a la UIAF.

XI. CAPÍTULO 11. USO MÓDULO RIESGOS EN EL APLICATIVO SVE

En el presente capitulo se dan orientaciones para el uso adecuado del aplicativo dispuesto para la creación y modificación de los riesgos gestionados en SVE, además de instrucciones para la materialización de los riesgos en el aplicativo. Esta explicación se realizará en referencia con las etapas de la gestión del riesgo.

Como generalidad dentro del aplicativo “Suite Visión Empresarial” los enlaces son los encargados de apoyar al responsable o líder en la realización de las acciones en el sistema para completar cada una de las etapas, contando con la aprobación y su respectivo soporte, para este caso la bitácora donde se encuentre el trabajo realizado de las mesas previas y la aprobación realizada por la **segunda línea de defensa.** En este orden de ideas toda creación o modificación. de riesgos debe ser solicitado por el responsable/líder del proceso o de la meta al jefe de la OAP o a la segunda línea de defensa (cuándo aplique), y los cambios deben quedar documentados en la bitácora de gestión del proceso/área. La Oficina Asesora de Planeación acompaña la revisión y aprobación de las tipologías de riesgos cuándo la segunda línea de defensa así lo solicite. La operación en el sistema se realiza posterior a contar con la revisión y aprobación del riesgo a crear o modificar.

Es de vital importancia aclarar que los roles en el aplicativo son netamente operativos del mismo, y en ningún caso exime de la responsabilidad de gestión del riesgo de los lideres o responsables de proceso en el marco del Sistema de Gestión del FONCEP y conforme al “Procedimiento para administrar los elementos de planeación y gestión institucional, PDT-EST-MIP-003".

Roles:

- Enlace: Realizar la propuesta del riesgo a crear o modificar, incluir en el sistema la información para la creación o modificación del riesgo según se haya aprobado (solicitud de apertura de etapas), formular acciones de tratamiento con los clasificadores correspondientes en el PAI, realizar monitoreo respondiendo las preguntas e incluyendo el comentario completo del mismo, materializar riesgos.

- Asesor o profesional de segunda línea asignado: Acompañar al proceso, área o líder de meta en toda la gestión de riesgos, realizar bitácora, aceptar la apertura de etapas adjuntando la bitácora de aprobación de la segunda línea de defensa, garantizar que los ajustes sean coherentes con lo establecido en el manual.
- Referente de riesgos: Realizar acompañamiento cuando es solicitado por el asesor o enlace, capacitar a colaboradores cuando la entidad lo solicite, revisar periódicamente el estado de los riesgos en el aplicativo verificando el cumplimiento de lo establecido en el manual, generar alertas a asesores, generar informes cuando le sean solicitado, realizar informe de segunda línea de defensa, publicar informes y mapas de riesgos y mantener el espacio virtual actualizado.
- Responsable y/o líder de proceso: revisar y aprobar las propuestas de creación y modificación del riesgo, solicitar a la segunda línea de defensa la aprobación de los cambios a realizar en los riesgos, confirmar información de monitoreo registrada por el enlace y solicitar la creación en el sistema de las acciones de tratamiento que se formulen

a) Identificación:

Para la creación del riesgo en el aplicativo, el enlace de cada proceso debe entrar al aplicativo en el "módulo de gestión de riesgo", pestaña "riesgos", y "gestionar"; en este punto debe ubicar el botón "crear" el cual también está señalado con el símbolo de suma (+)

En la ventana "identificación" diligencie los espacios obligatorios (los que tienen asterisco *) según las siguientes características:

- Nombre: sustantivo + verbo en participio + adjetivo, adverbio o complemento negativo. (*ejemplo: Procesos coactivos en contra del Foncep defendidos inadecuadamente).*
- Responsable: seleccione el nombre del enlace del proceso.
- Gestor: seleccione el nombre del responsable/líder del proceso.
- Descripción: describa el riesgo e indique información importante para comprensión del mismo. Específicamente delimite el alcance del riesgo o como se podría materializar operativamente hablando, establezca si se tiene un apetito del riesgo, describa el significado del nombre del riesgo en temas como a que se refiere el verbo participio o el adjetivo negativo del mismo. (*Ejemplo Posibilidad de recibir una dádiva o beneficio a nombre propio o de un tercero, al favorecer un proponente en el proceso de adjudicación de un contrato: Corresponde al momento cuando se compruebe que cualquier persona vinculada a la Entidad, reciba una dádiva o beneficio por crear, aprobar estudios previos que no estén basados en soportes legales, de mercado y según lo establecido en los procedimientos internos y lo establecido por la ley o que se adjudique un contrato cuando el proponente no cumple todos los requisitos).*
- Clase: seleccione de la lista desplegable el tipo de riesgo según corresponda.

- ¿Este riesgo es institucional? responda (Si o No) y justifique su respuesta. Los riesgos institucionales son los que por su importancia, impacto y característica general es considerado por la alta dirección como transversal a todo el FONCEP.
- ¿Este riesgo es de corrupción? responda (Si o No) y justifique su respuesta.
- Objetivos y áreas afectadas por el riesgo: con el botón "agregar" de cada pestaña (Objetivos estratégicos, Objetivos de proceso, Área organizativas) seleccione el elemento correspondiente de la lista y seleccione el botón "agregar y cerrar". Aplica para riesgos de proceso, seguridad de la información, corrupción; para los riesgos de metas no se incluye objetivo de proceso
- Causas y consecuencias del riesgo: con el botón "agregar" de la pestaña causa seleccione el factor generador y describa la causa, luego con el botón "agregar" de la pestaña consecuencia y escriba los impactos de la Tabla 8. Criterios para calificar el impacto según le aplique al riesgo.
- En el espacio de "información adicional" debe seleccionar el tipo de riesgo que identificó: Metas y resultados, Fiduciarios y financieros, Procesos (objetivos y salidas), Corrupción, Ambiental, Seguridad de la información, Seguridad y salud en el trabajo, Contractuales, SARLAFT, Finalice oprimiendo el botón "guardar" y "siguiente". Para el caso de riesgos estratégicos, no se debe establecer proceso, solo área responsable. En el espacio de "información adicional" debe seleccionar de la lista desplegable la meta a la cual apunta el riesgo.

Nota: Para todas las gestiones dentro de SVE debe quedar la trazabilidad de la bitácora con aprobaciones del jefe OAP o de la segunda línea de defensa (cuando aplique), específicamente, para la creación de un riesgo, la bitácora debe ser cargada por el enlace en la etapa de "análisis"

a) Análisis:

En la pestaña de "análisis" seleccione el nivel de probabilidad e impacto según lo dispuesto en la tabla 6 y tabla 8 del presente manual o en el link "+ Más información en rangos de Probabilidad" y "+ Más información en rangos de Impacto" seleccionando el criterio más alto de lo identificado y establecido en el paso anterior en el espacio de consecuencia.

Nota: Para los riesgos de corrupción en el análisis de impacto, el aplicativo muestra las 19 preguntas del DAFP; por tal razón se seleccionarán las pertinentes y el aplicativo generará automáticamente la escala de impacto.

Una vez realice esta acción, se mostrará el nivel de riesgo inherente al que corresponde el riesgo. Posteriormente, en el espacio "comentario" diligencie la acción realizada y una corta justificación o descripción del por qué seleccionó dichos criterios.

Cuando corresponda a un riesgo creado desde cero, en el espacio de comentarios se debe adjuntar la bitácora que soporta la aprobación de la creación del mismo.

Finalice oprimiendo el botón “guardar” y “siguiente”.

b) Evaluación y valoración.

En la pestaña de “valoración” seleccione “Controles para el riesgo”. En este espacio puede crear o utilizar controles ya creados a partir de los bonotes “nuevo” o “existente”.

En el caso que sea nuevo el control, se abrirá una ventana en la cual debe diligenciar los espacios obligatorios (los que tiene asterisco *) según las siguientes características:

- Nombre: Describa el propósito del control en infinitivo (ejemplo: garantizar, informar las características y tiempos de envío de información)
- Clase: Seleccione si el control es detectivo, preventivo o correctivo. Tenga en cuenta el verbo sugerido para la redacción del control para determinar cada clase y según se requiera para el control
- Escala afectada: Seleccione de la lista desplegable el tipo escala que afecta el control si es impacto, probabilidad. Recuerde que los controles preventivos y detectivos solo afectan probabilidad y los controles correctivos afectan impacto
- Descripción: Digite el control según lo descrito en el espacio de orientaciones técnicas para valoración de controles (responsable, periodicidad, propósito, cómo se realiza la actividad de control, qué pasa con las observaciones y desviaciones, evidencia)
- Causas: En el botón “agregar” puede seleccionar las causas ya identificadas en la etapa de identificación, posteriormente seleccione el botón “agregar y cerrar”.
- Consecuencias: En el botón “agregar” puede seleccionar las consecuencias ya identificados en la etapa de identificación, posteriormente seleccione el botón “agregar y cerrar”. Cuando se tiene un control correctivo se debe seleccionar el impacto que reduce, es decir, seleccionar la consecuencia exacta que se mitiga; cuando se tiene un control preventivo o detectivo se puede seleccionar todas las consecuencias.
- Proceso responsable: De la lista desplegable seleccione el proceso al que pertenece. No aplica para riesgos de meta y resultados
- Responsable: Automáticamente traerá el aplicativo su rol.
- Está documentado: responda si (Si o No) el control está en algún documento (procedimiento, manual, política, instructivo etc.) del sistema de gestión del FONCEP. Si su respuesta es sí seleccione el documento asociado.

Diligencie los espacios relacionados con atributos informativos:

- Documentación del control: Según la respuesta anterior de respuesta a) documentado o b) sin documentar
- Frecuencia del control: seleccione según aplique si es a) continúa o b) aleatorio.

- Evidencia de aplicación: según la descripción del control seleccione a) sin registro o b) con registro.

La evaluación del control se basa en dos preguntas que se responde con la descripción del control.

- Tipo de control: seleccione si es preventivo, detectivo o correctivo.
- Implementación del control: selecciones si es Automático o manual.

En otras palabras, responda las preguntas de evaluación de controles y atributos informativos según la realidad del proceso, metas y otros según aplique, posteriormente seleccione el botón “guardar” y luego en la ventana que se abre elija “cerrar”.

En el paso anterior, cerciórese de que el riesgo residual esté acorde con la calificación que les dio a los controles en la pestaña de “valoración”, de lo contrario comuníquese con el asesor OAP para tratar la incidencia. En esta pestaña en el espacio de “plan de contingencia” numere y describa las actividades a realizar cuando se le materialice el riesgo, esto solo para los riesgos extremos y se aconseja que estas no sean menos de tres (3) actividades.

Posteriormente, en el espacio “comentario” diligencie la acción realizada y una corta justificación o descripción de la valoración.

Finalice oprimiendo el botón “guardar” y “siguiente”.

c) Tratamiento (manejo)

En la ventana “manejo” seleccione una de las opciones de manejo. Recuerde que solo se permite aceptar los riesgos que se encuentren en zona de nivel bajo.

Si tiene que realizar acciones de tratamiento del riesgo, debe solicitar previamente su creación en el sistema siguiendo los lineamientos establecidos en el Manual para la formulación y seguimiento del plan de acción institucional MOI-EST-PES-003. Una vez creadas, en la pestaña “acciones asociadas” busque la categoría del área del plan de acción y oprima el botón “agregar y cerrar”

Despliegue el semáforo del riesgo con base en la selección de la opción “según la zona de riesgo” la lista desplegable

Seleccione la fecha del próximo monitoreo según el cronograma institucional.

Luego, en el espacio “comentario” diligencie la acción realizada y una corta justificación o descripción del manejo, posteriormente seleccione “siguiente”.

d) Monitoreo

Este paso estará dado por la acción del enlace y el responsable del proceso de acuerdo con las fechas establecidas en el cronograma institucional. Para esto en primera instancia el enlace debe:

- Revisar "Mis responsabilidades" en el módulo "Gestión del riesgo" y seleccionar el riesgo.
- Seleccionar el botón "Monitoreo",
- Debe iniciar en la pestaña "información adicional", dando respuesta a las preguntas que se encuentran en este espacio, a partir de estas deberá tomar decisiones para la gestión del riesgo en el próximo periodo (trimestre); en el espacio "observaciones" describa detalladamente la justificación de cada pregunta.
- En la pestaña "Registrar monitoreo", en el espacio "Comentario de monitoreo*" ingrese la información que diligenció en "observaciones" de cada uno de los criterios de evaluación (contexto, riesgo, controles y plan de tratamiento) del espacio "información adicional".
- En "archivos adjuntos" cargue las evidencias de controles. EJ: ID, Pantallas, GLPI.
- En el espacio "Fecha de próximo monitoreo*", ingrese la fecha y hora de finalización del monitoreo actual.

Ejemplo de monitoreo:

- *Observaciones de contexto: Durante el periodo no ha existido cambios impactantes relacionados con la normatividad que afecte el riesgo o los objetivos del proceso.*
- *Observaciones del riesgo: Durante el trimestre no se materializó este riesgo ni desde procesos de auditoría, ni de procesos de autoevaluación ya que no se crearon nuevos riesgos a los que ya tenía la entidad.*
- *Observaciones de los controles: Control 1: Garantizar la socialización de información institucional y del proceso importante a los colaboradores: El control se ejecutó, cada una de las áreas socializó información importante en el marco de sus comités primarios. Se adjunta documentos Excel con la información de comités y detalles de estos como número, fecha y ruta; Control 2: Asegurar la entrega de información y conocimiento de los elementos de planeación y gestión: El control se ejecutó de manera mensual, cada asesor OAP asignado apoyó a los enlaces, responsables y líderes en los temas asociados a riesgos, documentos, indicadores, plan de acción institucional y proyecto de inversión. Se adjunta una bitácora y pantalla de donde reposa la evidencia del control; Control 3. Validar la calidad y pertinencia de la asesoría: El control se ejecutó con corte junio 2022, se realizó la encuesta a los roles atendidos por la OAP, obteniendo los resultados que aportan a la mejora continua. Se adjunta la pantalla de la solicitud de la encuesta, y el indicador con el análisis respectivo.*
- *Observaciones de acciones de tratamiento: Este riesgo tiene dos actividades en el plan de acción: 1. Definir y ejecutar actividades a realizar para la implementación del mapa de aseguramiento en la Entidad. y 2. Realizar las intervenciones priorizadas en los elementos de gestión de los*

procesos que componen el mapa de procesos de la entidad. Trimestre II. Sobre la primera actividad se generó el documento sobre el impacto del mapa de aseguramiento. La segunda actividad fue finalizada donde se intervinieron diferentes procesos en las herramientas de gestión incluyendo los riesgos.

El responsable de proceso debe realizar las siguientes acciones:

- Revisar "Mis responsabilidades" en el módulo "Gestión del riesgo" y seleccionar el riesgo
- Seleccionar el botón "Monitoreo".
- Revisar la información incluida por el enlace.
  - En el espacio "Comentario de monitoreo*", si está de acuerdo con la información registrada, incluya un comentario de aprobación. Ej. "Fue revisada la información, la misma es pertinente y se aprueba el monitoreo"
  - En el espacio "Fecha de próximo monitoreo*", ingresar la fecha definida en el cronograma institucional.

e) Para solicitar modificación de cualquiera de las etapas de un riesgo ya creado:

El enlace debe buscar el riesgo en SVE, ubicarse en la etapa que desee modificar y dar clic en "Volver a Identificar/Analizar/Valorar/Manejar" según corresponda, es necesario incorporar una justificación de la modificación de la etapa indicando lo que se requiere ajustar. La solicitud llega a la segunda línea de defensa quien valida la justificación y que la misma corresponda a la modificación aprobada, de ser así se carga la bitácora que soporta la aprobación y acepta la apertura de etapa; de no cumplir los requisitos, la segunda línea no acepta la etapa y el enlace debe ajustar y realizar nuevamente la solicitud.

En cualquier momento la segunda línea de defensa o quien esta designe realiza la revisión del cargue adecuado del riesgo creado o modificado en el aplicativo SVE según lo aprobado, y emite recomendaciones para propender por la adecuada aplicación de los lineamientos definidos para cada tipo de riesgo y de su ciclo de gestión.

f) Materialización de riesgos.

Para generar una materialización, se debe ingresar al riesgo, ubicarse en la etapa de "Monitoreo" y en la parte inferior seleccionar el botón "Registrar evento". Se debe diligenciar los campos del formulario, los cuales se pueden responder a partir de la información diligenciada en el formato de análisis de causas.

CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DE LA MODIFICACIÓN
001	27 de julio de 2018	Se crea el y adopta el Documento con base en el Acuerdo de Junta Directiva No. 09 de 2018. Reemplaza el MOI-SIG-GRI003 Manual de Gestión del Riesgo.
002	09 diciembre de 2019	Actualización del manual según la guía de riesgos del DAFP
003	31 de agosto 2020	Actualización de manual en relación con la nueva política de gestión del riesgo, incluyendo la nueva tipología de riesgos en relación con la cadena de valor, inclusión de instructivo y pasos del manejo del Módulo riesgos SVE.
004	29 de octubre 2020	Se incluyeron recomendaciones generadas por la Secretaria de General, controles de riesgos, definición de roles de líneas de defensa, mejoras de definiciones de acciones para manejo de SVE, establecimiento de definiciones.
005	Diciembre de 2020	Se incluyen los lineamientos para la gestión de riesgos contractuales emitidos por la segunda línea de defensa
006	Marzo de 2021	Se incluye la metodología para el monitoreo de los riesgos contractuales definiendo el muestreo, periodicidad y actualización de la matriz de monitoreo de los riesgos.
007	Marzo de 2021	Se incluye lineamiento sobre riesgos fiduciarios.
008	Mayo de 2021	Se define características de los informes de segunda línea de defensa en el marco del rol y funciones de esta línea y se integra el paso a paso a realizar cuando se materializa un riesgo contractual
009	Julio de 2021	Se amplían instrucciones para las definiciones sobre riesgos fiduciarios
010	Agosto de 2021	Se incluye lineamiento sobre riesgos de Lavado de Activos y Financiación del Terrorismo. Se establecen lineamientos para identificar riesgos además de acciones a realizar cuando el riesgo no tiene controles
011	Octubre 2021	Se incluyen los elementos relacionados con la guía DAFP versión 5 2020 y la actualización del aplicativo SVE, la cual afecta política, identificación, análisis y valoración de riesgos. Adicionalmente se actualizan documentos asociados en seguridad de la información y ambiental. En riesgos contractuales se ingresa la etapa de liquidación.
012	Agosto 2022	Se amplía la información el Capítulo 5. Riesgos de seguridad información. Se actualizan líneas de defensa según evaluación de IDI para dar cumplimiento a los requisitos evaluados. Se actualiza forma de cargue en SVE y responsabilidades. Se agregan elementos para definir nombre y descripción de riesgos. Se crea capitulo de uso de módulo de riesgos en SVE.

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Joaquín Manuel Granados Rodriguez **Enlace del proceso** Profesional especializado OAP-Contratista OAP Edilberto Forero Vivas **Enlace del proceso** Profesional especializado-Contratista OAP María del Pilar Segura González **Enlace del proceso** Profesional – Contratista OIS	Cristian Mauricio Amaya Martínez **Responsable de proceso** Jefe de la Oficina Asesora de Planeación Carlos Enrique Fierro Sequera **Responsable del proceso** Jefe de la Oficina Asesora de Jurídica Wilson Barrios Delgado **Responsable del proceso** Jefe de la Oficina de Informática y Sistemas Jenny Andrea Ramírez Oviedo **Asesor OAP** Profesional especializado -Contratista OAP	Cristian Mauricio Amaya Martínez **Líder del proceso** Jefe de la Oficina Asesora de Planeación