Superintendencia Financiera de Colombia

Metodología de Riesgos

E-ME-PLA-001
Versión 4
Noviembre, 2022

CONTENIDO

INTRODUCCIÓN

La Superintendencia Financiera de Colombia dando cumplimiento a lo establecido por el 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 y de acuerdo con los lineamientos del Sistema de Gestión Integrado de la Entidad, se compromete a mejorar continuamente la prestación del servicio para el beneficio de la Entidad y sus usuarios con la implementa el modelo para la gestión y administración de riesgos sugerido por la Guía para la Administración del Riesgo y el Modelo de administración de Controles con referencia de las guías definidas para las Entidades Públicas por el Departamento Administrativo de Función Pública (DAFP) - Riesgos de gestión, corrupción y seguridad digital.

El riesgo como elemento inherente a las actividades propias de organización, es considerado dentro del Sistema de Gestión Integrado de la Superintendencia Financiera de Colombia (SFC). La Gestión de Riesgos en la Entidad busca generar valor agregado a las actividades desarrolladas, mejorar el desempeño de los procesos, fomentar la innovación y contribuir en la consecución de objetivos.

Los riesgos emergentes originados a partir de la globalización, las catástrofes naturales, atentados terroristas y acontecimientos inesperados, las crisis financieras, los nuevos entornos regulatorios a nivel internacional, la innovación tecnológica, la creación de nuevos productos y/o metodologías, exigen a las entidades una adecuada y oportuna gestión del riesgo.

El presente documento comprende la identificación, valoración y evaluación de los riesgos para cada proceso, así como la definición de actividades de control que permitan mitigar la probabilidad de ocurrencia y/o impacto de los mismos.

Para la definición de la presente metodología de riesgos se consideraron los siguientes estándares internacionales y nacionales:

a. Nivel internacional

- NTC ISO 31000 Gestión del Riesgo Principios y Directrices: Modelo estándar para la gestión de riesgos.
- Comité COSO: Define la administración de riesgos como uno de los elementos claves del sistema de control y emite la versión de ERM como modelo a seguir.
- ISO/IEC 27032 Sistema de Gestión de Ciberseguridad
- ISO 22316 Resiliencia Organizacional
- NTC ISO 27001 Sistema de Gestión de Seguridad de la información.
- NTC ISO 22301 Sistema de Gestión de Continuidad del Negocio.

- Principios del Comité de Basilea: Propicia en las entidades bancarias la administración de riesgos.
- Ley Sarbanes Oxley: Responsabiliza a la dirección de reportar sobre el establecimiento y mantenimiento de una estructura de control interno.

b. Nivel nacional

- Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas del Departamento Administrativo de Función Pública (DAFP).
- Modelo Integrado de Planeación y Gestión (MIPG): Aplicado a las entidades del estado colombiano, que incluye el componente administrativo de riesgos como parte integral del sistema de control.

Para la gestión integral de riesgos, se implementa el modelo ERM (Enterprise Risk Management) el cual es un proceso que permite tratar eficazmente la incertidumbre, identificando los riesgos y las oportunidades, y optimizando la capacidad de generar valor. Usa un enfoque común para evaluar los riesgos dentro de la Entidad, que permita integrar la discusión de riesgos dentro de la planificación estratégica y táctica, la asignación presupuestal, gestión del desempeño y en otros procesos, para la toma de decisiones diaria.

El uso de análisis de escenarios y simulaciones dinámicas puede respaldar la planificación estratégica al analizar las probabilidades y los resultados de diferentes estrategias organizacionales, así como el impacto potencial en las partes interesadas. Así mismo, las lecciones aprendidas pueden ser aprovechadas para la planificación estratégica futura y los planes de respuesta a los nuevos riesgos que puedan surgir.

ERM apoya la misión de la Entidad, gestionando los riesgos de manera integral, estableciendo alertas tempranas y priorizando los riesgos. La priorización de los riesgos deberá considerar entre otras, las causas fundamentales, las fuentes, la probabilidad y los posibles resultados positivos.

La Alta Dirección debe tomar una decisión estratégica sobre el estilo, la forma y la calidad de la administración de riesgos y debe liderar la evaluación y gestión de oportunidades y riesgos, considerando los requisitos y restricciones que influyen en la priorización de los recursos, tales como las preocupaciones de política, las necesidades de la misión, los intereses y prioridades de las partes interesadas, la cultura y el nivel de aceptación.

Por otro lado, los directivos deben determinar y evaluar continuamente la naturaleza y el alcance de los principales riesgos a los que la organización está expuesta y está dispuesta a asumir para lograr sus objetivos (su apetito por riesgo) y asegurarse de que la planificación y la toma de decisiones reflejen esta evaluación.

1. CONTEXTO ORGANIZACIONAL SUPERINTENDENCIA FINANCIERA DE COLOMBIA

La Superintendencia Financiera de Colombia, es un organismo técnico adscrito al Ministerio de Hacienda y Crédito Público, con personería jurídica, autonomía administrativa y financiera y patrimonio propio, a través de la cual, el Presidente de la República, de acuerdo con la ley, ejerce la inspección, vigilancia y control sobre las personas que realizan actividad financiera, bursátil, aseguradora y cualquier otra relacionada con el manejo, aprovechamiento o inversión de recursos captados del público.

De acuerdo con la evaluación técnica adelantada por el Ministerio de Hacienda y Crédito Público y aprobada por el Departamento Administrativo de la Función Pública, la Superintendencia Bancaria y la Superintendencia de Valores, fueron fusionadas mediante el Decreto 4327 de 2005, la cual en adelante se denomina Superintendencia Financiera de Colombia.

La Entidad ejerce las funciones establecidas en el Decreto 2739 de 1991 y demás normas que la modifiquen o adicionen; el Decreto 663 de 1993, la Ley 964 de 2005 y demás normas que la modifiquen o adicionen, las demás que señalen las normas vigentes y las que le delegue el Presidente de la República.

Para asegurar la disponibilidad de las herramientas y el talento humano necesario para cumplir a cabalidad con las funciones y el propósito de esta, los procesos de la Entidad basados en el ciclo PHVA (Planear, hacer, Verificar y Actuar) garantizan que los recursos que se necesitan para dar cumplimiento a sus funciones estarán a disposición en el lugar y el momento en que se requieran.

Así mismo, el proceso la Entidad cuenta con el proceso de Gestión Documental para administrar la documentación que se reciba o se produzca en la Entidad, con el fin de garantizar su disponibilidad, almacenamiento, conservación y disposición final, de acuerdo con lo establecido en las Tablas de Retención Documental, y demás normas vigentes relacionadas con el tema.

Es así como, la Entidad, apoyada en las mejores prácticas nacionales e internacionales, formula diferentes proyectos, programas, estrategias y/o planes que conducen a estar mejor preparada para enfrentar las vulnerabilidades propias del entorno.

De igual manera, considera la adopción de mejores prácticas en materia de gestión y análisis de riesgos, requerimientos prudenciales, supervisión tanto de las entidades del sistema financiero como de los conglomerados financieros, mecanismos de resolución, racionalización y mejoramiento de requerimientos y condiciones, entre otros, que incentiven el acceso al sistema financiero.

Para dar cumplimiento a la planeación estratégica es necesario fortalecer la cultura institucional que a lo largo de los años ha distinguido a la Superfinanciera, por su alta calidad técnica, el estricto cumplimiento de la ley en el ejercicio de sus funciones y cero tolerancias frente a la corrupción.

Los integrantes de la Superfinanciera asumen y se comprometen con los valores y principios generales de los servidores públicos colombianos contenidos en el documento "Valores del Servicio Público – Código de Integridad" y establecidos a nivel interno en el Código de Integridad SFC (A-CO-GTH-001).

Su propuesta de valor se centra en un sistema financiero que sea innovador, eficiente y consolidado mediante la oferta de un servicio adecuado por medio de la adopción de nuevas tecnologías. Lo anterior se logra a través de la definición de pilares que determinan la actividad de supervisión, normativa, de protección al consumidor financiero y la labor administrativa de la Entidad con el fin de tener un sistema financiero competitivo, sostenible, incluyente y confiable.

2. GRUPOS DE VALOR DE LA SUPERINTENDENCIA FINANCIERA DE COLOMBIA

Para crear valor y asegurar el éxito de las organizaciones a largo plazo, se debe crear y mantener una relación sólida con los diferentes grupos con los que interactúa la Entidad, en un entorno de respeto mutuo, diálogo abierto, identificación de necesidades, búsqueda del mutuo beneficio y apertura al cambio, con personas bien preparadas, competentes, motivadas e interesadas en el bien común.

Los grupos de valor son considerados un elemento esencial en el ejercicio de planeación estratégica. Para la Superfinanciera, los grupos de valor están conformados por todas aquellas personas o entidades que se puedan ver beneficiadas por las actividades que realiza la Entidad, dentro de los cuales se destacan principalmente el Consumidor Financiero, las Entidades Vigiladas, y las otras partes interesadas que incluyen al Gobiernos, Asociaciones, Organismos multilaterales, Academia, Medios de comunicación.

3. OBJETIVOS

El presente documento se desarrolla con el fin de relacionar los elementos básicos a tener en cuenta para lograr una gestión de riesgos eficaz y eficiente, que contribuya con la toma de decisiones y el logro de los objetivos institucionales.

Los objetivos principales que busca alcanzar la presente metodología son:

- Garantizar el cumplimiento de los objetivos institucionales a través de la adecuada gestión de los riesgos.
- Generar una cultura de administración y control de riesgos al interior de la Entidad en la que se involucre a todos los funcionarios en las acciones encaminadas a la reducir o mitigar los efectos de la materialización de los riesgos.

- Asegurar la continuidad de la operación en la Entidad ante escenarios adversos.
- Proteger los activos de la organización resguardándolos contra la materialización de los riesgos.
- Robustecer la calidad de los procesos y procedimientos con acciones de prevención y mitigación de riesgos.
- Asegurar el cumplimiento de normas, leyes y regulaciones en materia de gestión de riesgos.
- Integrar la gestión de los riesgos con temas como los riesgos de corrupción, los riesgos en seguridad de la información, la continuidad del negocio, los riesgos de ciberseguridad y la identificación de terceros (lavado de activos y financiación del terrorismo).
- Generar información clara, oportuna y útil para la toma de decisiones de las partes interesadas.

4. ALCANCE

La presente metodología involucra a todos los funcionarios de la entidad y es aplicable a todos los procesos del Sistema de Gestión Integrado de la Superintendencia Financiera de Colombia, con el propósito de apoyar la toma de decisiones en materia de los riesgos a los que pueda estar expuesta de forma tangible o intangible y facilitar el cumplimiento de los objetivos previamente mencionados, así como también de aquellos considerados estratégicos para la organización, con lo que se espera mitigar los impactos negativos que puedan afectarla mediante la utilización de las herramientas tecnológicas y el conocimiento que aporta su talento humano. La revisión de la metodología se hará anualmente o cada vez que se identifiquen cambios en los riesgos o en la normatividad aplicable a la misma.

5. INSTITUCIONALIDAD

El Modelo Integrado de Planeación y Gestión (MIPG) define la creación en todas las entidades públicas del Comité Institucional de Gestión y Desempeño, regulado por el Decreto 1499 de 2017 y el Comité Institucional de Coordinación de Control Interno, reglamentado a través del artículo 13 de la Ley 87 de 1993 y el Decreto 648 de 2017, para contribuir con la adecuada gestión del riesgo.

La alineación de la Gestión de Riesgo con MIPG se desprende de la dimensión de Direccionamiento Estratégico y Planeación, en la cual se generan los lineamientos para administración de riesgos de la línea estratégica de defensa definida en la Dimensión de Control Interno.

5.1 Comité institucional de Gestión y Desempeño

En este Comité se analiza la gestión del riesgo con base en el seguimiento periódico y se generan las mejoras para fortalecer la administración del riesgo en la Entidad.

5.2 Comité institucional de Coordinación de Control Interno

En este Comité se presenta el análisis de los eventos y los riesgos críticos identificado durante la fase de seguimiento y monitoreo.

5.3 Lideres de proceso

Los líderes de proceso son los responsables de la identificación, valoración, control y monitoreo de los riesgos, en la primera línea. Mínimo una vez al año, se deberá realizar la revisión integral de la administración de riesgos.

5.4 Segunda línea de defensa

Es responsabilidad de la Oficina Asesora de Planeación, a través del Grupo de Resiliencia Operacional, actuar como segunda línea de defensa frente a la gestión de riesgos. Las funciones que desempeña se encuentran definidas en el Modelo De Gobierno Resiliencia Operacional (E-MN-PLA-006), no obstante, frente a la gestión de riesgos debe:

- ✓ Coordinar el proceso de gestión y administración del riesgo, bajo las orientaciones de la Alta Dirección.
- ✓ Capacitar a los servidores de la Entidad en la administración y gestión de los riesgos.
- ✓ Asesorar a las áreas de la Entidad y a los funcionarios designados para la gestión del riesgo.
- ✓ Revisar, analizar y consolidar la información para presentar propuestas de correctivos y/o mejoras de los dominios de resiliencia operacional a la Alta Dirección.
- ✓ Gestionar con los funcionarios responsables (Coordinadores de proceso, Grupo de Resiliencia Operacional, Lideres, Facilitadores y Enlaces), la alineación de actividades enfocadas en la administración de riesgos y ejecución de controles.
  Construir un inventario de controles de riesgos para toda la Entidad, a partir de las actividades de control definidas por cada proceso que compone el Sistema de Gestión Integrado, con el fin de medir la efectividad de estos en la mitigación del riesgo.

5.5 Funcionarios

Son las personas responsables de ejecutar los controles en la operación diaria de la Entidad.

6. METODOLOGÍA PARA LA GESTIÓN DEL RIESGO

La gestión de riesgos en la Entidad se realiza con base en los lineamientos definidos por el Departamento Administrativo de la Función Pública-DAFP, quien a su vez toma como referencia conceptual los criterios establecidos en la norma ISO 31000 de 2018.

Diagrama 1. - Fases de la Metodología de Riesgos

Fuente: ISO 31000 y DAFP

Como apoyo para la implementación de la metodología de riesgos en la Entidad, se cuenta con la proforma interna E-PI-PLA-018-Plantilla Contexto Organizacional y Matriz de Riesgos.

6.1 CONOCIMIENTO Y CONTEXTO DE LA ENTIDAD

Dentro de los criterios que se deben considerar para realizar un análisis completo de la Entidad se encuentran el conocimiento de los objetivos estratégicos, la misión, la visión, la planeación estratégica y la caracterización de los procesos (cadena de valor, mapa, planes, proyectos). Así mismo, se requiere identificar el estado actual de los riesgos y la gestión de estos.

a) Cadena de valor

Corresponde a la identificación de interrelaciones entre los procesos y actividades que componen el Sistema de Gestión Integrado de la Entidad.

b) Mapa de procesos

El modelo de operación por procesos es el estándar organizacional que soporta la operación de la Entidad, integrando las competencias constitucionales y legales que la rigen con el conjunto de planes y programas necesarios para el cumplimiento de su misión, visión y objetivos institucionales. El mapa de procesos es la representación

gráfica de la cadena de valor de los procesos de la Entidad. La Superintendencia Financiera de Colombia cumple con los requisitos de la ISO 9001, en esta materia.

c) Caracterización de los procesos

Estructura que permite identificar las características de cada proceso basado en el ciclo PHVA (planear, hacer, verificar y actuar), identificando el objetivo, los proveedores, las entradas, las actividades, las salidas y los clientes.

d) Relación objetivos estratégicos, misión, visión, planeación estratégica y la gestión de riesgos

La Entidad debe analizar los objetivos estratégicos y revisar que se encuentren alineados con la misión y la visión institucionales, así como su desdoble hacia los objetivos de los procesos, teniendo en cuenta el aporte que la gestión de riesgos tiene en la toma de decisiones, protegiendo los recursos de la Entidad, mejorando los resultados y optimizando la prestación de servicios a sus usuarios. Así mismo, fortalece el ejercicio del Control Interno en la Entidad.

e) Matriz y estrategias DOFA

Es la herramienta dispuesta para identificar el análisis de contexto para cada uno de los procesos del SGI, la cual identifica las debilidades, oportunidades, fortalezas y amenazas de este y su incidencia en los objetivos estratégicos de la Entidad.[1]

Es importante considerar que para realizar el análisis interno del proceso se deben identificar las debilidades y fortalezas de este, las cuales hacen referencia a los factores negativos que lo afectan y a los factores positivos que permiten mantener la solidez del proceso, respectivamente.

Por su parte, para realizar el análisis externo se debe considerar las oportunidades y amenazas del proceso, las cuales correspondes a las características externas que pueden conducir a la adopción de nuevas posibilidades deseables y viables para abordar las necesidades del proceso y sus partes interesadas y a los factores externos que pueden suponer riesgos para el proceso, respectivamente.

Una vez definidos los cuatro (4) elementos que constituyen la matriz DOFA, se deben formular al menos una estrategia para cada una de las interacciones que componen la matriz (FO-FA-DO-DA)[2]. Es posible tomar la relación de más de una fortaleza o debilidad con más de una oportunidad o amenaza.

De acuerdo con las interacciones entre los elementos de la matriz DOFA y el objetivo que cada una de estas persigue, se sugieren los siguientes tipos de estrategias:

[1] La herramienta definida para la construcción de la matriz es la proforma interna E-PI-PLA-018- hoja “A. DOFA”.
[2] Las estrategias DOFA se deben relacionar en la proforma interna E-PI-PLA-018- hoja B. ESTRATEGIAS DOFA.

a. Estrategia de Reorientación (Debilidades-Oportunidades): Acciones para corregir las debilidades con las oportunidades del proceso.
b. Estrategias de ataque (Oportunidades-Fortalezas): Acciones para explotar las oportunidades con las fortalezas del proceso.
c. Estrategias de supervivencia (Amenazas-Debilidades): Acciones para afrontar las amenazas derivadas de las debilidades del proceso.
d. Estrategias Defensivas (Fortalezas- Amenazas): Acciones para mantener las fortalezas del proceso buscando eliminar las amenazas.

A continuación, se describen los criterios estratégicos y operativos, mínimos, que se deben considerar para la definición y redacción de las estrategias DOFA:

- Debe iniciar con un verbo en infinitivo, que describa la acción a realizar.
- Debe contener el propósito y/o impacto de la actividad a desarrollar.
- Debe contener el valor agregado que genera para el proceso o a la Entidad.
- Se debe indicar la fecha máxima de ejecución, la cual no debe ser superior a un (1) año posterior a la actualización de la matriz de riesgos.
- Debe definir cuál la evidencia de su ejecución y/o entregable.
- Debe definir el funcionario o cargo responsable de liderar su ejecución.

Cada estrategia DOFA deberá estar relacionada con un proyecto, programa o plan de mejora con el fin de realizar el respectivo seguimiento a los avances. En caso de no estar relacionada con ninguno de los anteriores, se deberá considerar dentro de las actividades del plan de acción que se defina para la gestión de riesgos[3].

Adicionalmente, para apoyar la identificación del contexto, el proceso puede considerar, entre otras, la siguiente información:

- Amenazas y vulnerabilidades cibernéticas.
- Análisis DOFA del proceso.
- Caracterización del proceso.
- Consumidores financieros, clientes, o entidades o agentes económicos involucrados (Grupos de Valor, clientes y partes interesadas, etc.).
- Datos estadísticos de ejecución de los productos de los procesos.
- Indicadores de gestión y cumplimiento de metas.
- Informes de auditoría de gestión, de calidad o de entes externos.
- Inventario de activos de información.
- Lineamientos estratégicos de la Entidad, incluidos los objetivos estratégicos.
- Mapa de procesos y la interacción con otros procesos (E-MA-PLA-002 Matriz interrelación de Procesos).
- Matriz de riesgos vigente.
- Normativa.
- Planes de acción y sus resultados.
- Principales documentos o registros que intervienen en las operaciones, cuál es la función que cumplen, quienes los originan, quienes los reciben etc.

[3] En el ítem "Tratamiento de riesgos" se definen los criterios para crear la oportunidad de mejora con el fin de gestionar el riesgo.

- Quejas de usuarios contra las entidades vigiladas y PQRSF.
- Registros que evidencien la ejecución, responsabilidad. frecuencia, como se realiza, desviaciones y efectividad de los controles.
- Reportes de materialización de riesgos y el tratamiento.
- Reportes de no conformidades y salidas no conformes.
- Expectativas y necesidades de las partes interesadas.

6.2 POLÍTICA DE RIESGOS

La Entidad cuenta con la Política Institucional de Gestión de Riesgos la cual define los compromisos y objetivos de la Entidad frente a la gestión integral, oportuna y adecuada en la administración de sus riesgos, alineada con la misión, visión y objetivos estratégicos de la Alta Dirección.[4]

6.2.1 Lineamientos Generales en la Gestión de Riesgos

La gestión de riesgo se realiza de manera integral y estructurada teniendo en cuenta todas las actividades definidas para el cumplimiento de la misión y los objetivos estratégicos de la Entidad, dando un enfoque exhaustivo al análisis de resultados que permitan identificar acciones a implementar.

Es fundamental, previo a la implementación de la presente metodología, considerar el análisis de contexto interno y externo de acuerdo con los objetivos estratégicos de la Entidad y del proceso, con el fin de adaptar la gestión del riesgo de acuerdo con los resultados obtenidos.

Durante el análisis de contexto, es necesario contemplar el propósito y la planeación estratégica de la Entidad, considerando el entorno en donde se desarrolla la actividad de la organización a nivel social, económico, cultural, ambiental, tecnológico, entre otros. De esta forma, se identifican las capacidades para lograr los objetivos estratégicos de la Entidad. El líder del proceso con su equipo de trabajo debe revisar la documentación definida por cada proceso, así como los lineamientos del Plan Estratégico de la Entidad, el cual se encuentra consignado en el sitio web de la Entidad.

Adicionalmente, se debe considerar la participación de las partes interesadas (internas y externas), identificadas en cada proceso, enfocada en obtener diferentes puntos de vista que permitan una mayor comunicación de la gestión de riesgos. Así mismo, se deben considerar la información contenida en el documento Matriz Comprensión de Necesidades y Expectativas Partes Interesadas.[5]

El resultado del análisis de contexto permite identificar los cambios en los riesgos, con el fin de evaluar la inclusión de nuevas amenazas y mantener o eliminar los identificados en la matriz de riesgos vigente. Dicho ejercicio se realiza como mínimo

[4] Se encuentra oficializada en el aplicativo SGI bajo el código E-PT-PLA-009.

[5] Se encuentra oficializada en el aplicativo SGI bajo el código E-MA-PLA-017.

una vez al año, al momento de actualizar las matrices de riesgos, permitiendo una gestión de riesgo dinámica, que cuente con información actualizada y oportuna para la toma de decisiones por parte de los procesos y las partes interesadas. El resultado de este análisis se refleja en los reportes de gestión de riesgo presentados periódicamente.

Como resultado de la aplicación de la metodología establecida en el presente documento, se refleja en el diligenciamiento y oficialización en el aplicativo SGI de la Plantilla Contexto Organizacional y Matriz de Riesgos, la cual permite identificar la implementación de cada una de las fases definidas para la adecuada gestión de los riesgos por cada proceso.

Como medio para contribuir con el logro de los objetivos, se establecen actividades de control orientadas a prevenir y mitigar la materialización de los riesgos. Le corresponde a la primera línea de defensa el establecimiento de actividades de control relacionadas con los riesgos inherentes a las actividades que desarrolla y a la segunda línea las relacionadas con continuidad y ciberseguridad.

El producto de la actualización de las matrices de riesgos de cada uno de los procesos del Sistema de Gestión Integrado, se generan los mapas de riesgos de la Entidad, los cuales, luego de ser revisado y aprobado en el aplicativo SGI, se proceden a generar la versión oficial para publicación en el sitio web de la Entidad. Así mismo, se establece el perfil de riesgo y se revalúa o ratifica el apetito por riesgo de la Entidad.

De igual manera, para la gestión de riesgos el factor humano es un recursos indispensable para su desarrollo, por lo anterior, se cuenta con un plan de capacitación y sensibilización continua enfocado en establecer la cultura de riesgos y control en toda la Entidad, la cual refleja sus valores, comportamientos y decisiones, de acuerdo con la transmisión de la información, generando juicios de valor, capacidades y experiencia disponibles que fomenten la imparcialidad y establecimiento de valores claves para la gestión de riesgos.

Teniendo en cuenta lo anterior, cada proceso debe realizar análisis, valoración y actualización de riesgos de acuerdo con los lineamientos definidos en el presente documento, de tal manera que se identifique e implemente los componentes del marco de referencia que garanticen el éxito de la gestión integral de los riesgos.

El funcionario designado para resolver los conflictos de interés y las incertidumbres frente a la implementación de la presente metodología de riegos es el Jefe de la Oficina Asesora de Planeación y/o Líder del proceso de Planeación, quien realizará el análisis y definirá las recomendaciones pertinentes para el logro de soluciones efectivas.

6.2.2 Niveles de aceptación al riesgo

La Gestión de Riesgos en la Entidad busca generar valor agregado a las actividades que desarrolla, mejorar el desempeño de los procesos, fomentar la innovación y

contribuir en la consecución de metas, por lo que requiere que sus estrategias están alineadas con su apetito por riesgo, el cual corresponde al nivel de riesgo que la Entidad quiere aceptar y con el cual se siente cómoda para conseguir sus objetivos.

Teniendo en cuenta que el nivel de riesgo es considerado como la combinación entre la probabilidad de ocurrencia y el impacto de este, es importante definir previamente el nivel de apetito por riesgo y el nivel de tolerancia al riesgo (desviación respecto al apetito por riesgo, que representa una alerta para evitar llegar a la capacidad). Así mismo, conocer la capacidad de riesgo (nivel máximo de riesgo que la Entidad puede soportar), para definir estrategias alternas que se alineen con la misión, visión, objetivos estratégicos y valores claves de la organización.

Dichos niveles son definidos y actualizados por la Alta Dirección, considerando el perfil de riesgos de la Entidad, los cambios en el contexto organizacional y el plan estratégico, al menos una vez al año.

El perfil de riesgos es el resultado de agregar y promediar las variables probabilidad de ocurrencia e impacto de los riesgos identificados y evaluados en los 21 procesos del SGI, los cuales se determinar el nivel de riesgo para la Entidad, con el fin de proporcionar una vista compuesta del riesgo que enfrenta, permitiendo considerar la severidad, el tipo, la interdependencia entre los riesgos y la afectación sobre el logro de los objetivos.

6.3 IDENTIFICACIÓN DEL RIESGO

El riesgo es la posibilidad de incurrir en pérdidas por eventos potenciales, relacionados con las deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos, que generen un efecto negativo sobre los objetivos de la Entidad.

La identificación del riesgo debe contemplar todas las amenazas, situaciones o actos que puedan causar daño a los objetivos del proceso y/o de la Entidad, estén o no bajo el control de esta.[6]

El primer elemento para la identificación de los riesgos inherentes al proceso es el resultado del análisis de contexto y matriz DOFA. En esta fase el proceso deberá considerar todas las actividades definidas para cada subproceso con el fin de tener un contexto mucho más amplio para la identificación de riesgos.

Para iniciar con la definición de los riesgos se debe entender plenamente el objetivo del proceso, con el fin de identificar los posibles eventos de riesgo que afecten el logro de este, cuestionándose sobre:

[6] La identificación y caracterización de los riesgos del proceso se realiza en la proforma interna E-PI-PLA-018- hoja "C.RIESGOS".

- **¿Qué puede suceder?** Identificar los efectos del cumplimiento del objetivo estratégico o del proceso según sea el caso.
- **¿Cómo y porqué puede suceder?** Establecer las causas a partir de los factores determinados en el contexto.
- **¿Cuándo puede suceder?** Determinar el momento o la etapa en que puede ocurrir de acuerdo con el desarrollo del proceso.
- **¿Qué consecuencias tendría su materialización?** Determinar los posibles efectos por la materialización del riesgo.

Es importante preguntarse si el riesgo identificado está relacionado directamente con las características del objetivo. Si la respuesta es "No" éste puede ser la causa o la consecuencia del riesgo.

En el análisis que realice para identificar los riesgos contemple en primer lugar los riesgos que ya se han materializado.

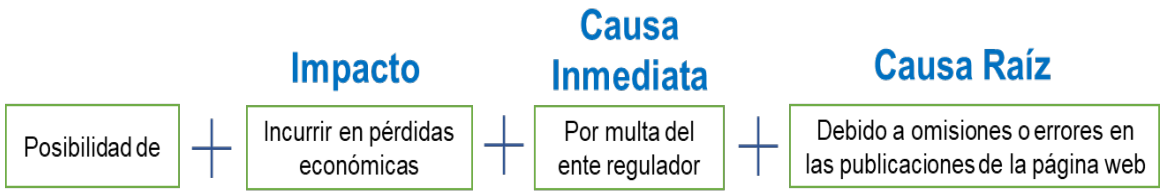
Para realizar la identificación única del riesgo en toda la Entidad, se debe registrar el código del riesgo, en el campo "ID_Riesgo" de la hoja C. RIESGOS de la proforma interna. Dicho código debe seguir la siguiente estructura:

- Identifique el código del riesgo con las siglas del proceso en el SGI. Ejemplo: PLA, SEG, AUT, FJU, etc.
- Complemente con un consecutivo de tres dígitos. Ejemplo: PLA_001, AUT_003, FJU_015, etc.

6.3.1 Descripción del riesgo

Para la descripción del riesgo se debe considerar todos los detalles que sean necesarios para que sea de fácil entendimiento a personas ajenas al proceso. La estructura que se debe seguir para su redacción es la siguiente: Inicia con la frase "Posibilidad de" + Impacto + Causa Inmediata + Causa Raíz.

Ejemplo:



Impacto (¿qué?): Son las consecuencias que puede ocasionar la materialización del riesgo. Ejemplo: Pérdida Económica y/o Reputacional.

Causa Inmediata (¿cómo?): Corresponde las circunstancias o situaciones que generan el impacto. Ejemplos: Multas, sanciones, afectación a la imagen institucional.

Causa Raíz (¿por qué?): Es la causa principal por la cual se puede presentar la causa inmediata. Ejemplo: Inoportunidad en la entrega de productos y/o servicios, reprocesos en la información, actos malintencionados de los funcionarios.

Adicionalmente, se debe complementar, para finalizar la redacción del riesgo, la identificación del punto a partir del cual se establece existe la materialización del riesgo. Ejemplo: El riesgo se materializa cuando producto del reproceso de información se reciba una queja y/o inconformidad por parte del destinatario. El riesgo se materializa cuando se presente el X% de productos entregados inoportunamente en el mes. El riesgo se materializa a partir del incumplimiento del indicador XXX o cuando se presenten dos o más productos no conformes durante el mes.

6.3.2 Caracterización del riesgo

Con el fin de identificar los elementos que permiten evaluar y clasificar el riesgo, se realiza la caracterización del riesgo considerando los siguientes aspectos:

6.3.2.1 Análisis de objetivos estratégicos y de los procesos

El análisis de objetivos estratégicos y de los procesos es importante teniendo en cuenta que todos los riesgos que se identifiquen deben afectar el cumplimiento de estos. Se deben considerar los siguientes aspectos para que este análisis sea exitoso:

- Coherencia del objetivo del proceso con la misión y la visión de la Entidad.
- Revisión de objetivos estratégicos y de los procesos, teniendo en cuenta que estos deben estar alineados a la misión, visión y propósito superior; deben incluir el qué, cómo, para qué, cuándo, cuánto y deben contemplar al menos las siguientes características: sean específicos, medibles, alcanzables, relevantes y proyectados en el tiempo.[7]

6.3.2.2 Identificación de los puntos de riesgo

Son las actividades de cada proceso en las cuales existe evidencia o se tiene indicios que puede ocurrir eventos de riesgo que afecten el cumplimiento de sus objetivos y por tanto, requieren tenerse bajo control para asegurar que el proceso cumpla con las metas definidas.

6.3.2.3 Identificación de áreas de impacto

La definición de las áreas de impacto hace referencia a la consecuencia económica y/o reputacional a la que se ven expuestos los procesos ante la materialización del riesgo.

[7] Le corresponde a la Oficina Asesora de Planeación la revisión de los objetivos de la Entidad tanto del orden estratégico como de los procesos, entre sus funciones de calidad, con el fin de que se encuentren definidos correctamente.

6.3.2.4 Identificación de áreas de factores de riesgo

Son las fuentes originadoras de riesgos que pueden o no generar pérdidas.[8] Para la Entidad se identifican los siguientes factores de riesgos:

- **Procesos:** Eventos relacionados con errores en las actividades que deben realizar los funcionarios de la Entidad (falta de procedimientos, error humano, falta de capacitación, etc.).
- **Talento Humano:** Eventos relacionados con actos con posible dolo e intención hacia actos indebidos (corrupción, soborno, falta de ética, etc.). Adicionalmente, se relaciona con eventos asociados a la seguridad y la salud en el trabajo.
- **Tecnología:** Eventos relacionados con la infraestructura tecnológica de la entidad (software, hardware, telecomunicaciones, etc.).
- **Infraestructura:** Eventos relacionados con la infraestructura física a causa de desastres naturales o daños a activos fijos de la Entidad (inundaciones, incendios, etc).
- **Eventos externos:** Hace referencia a las actividades o eventos externos que no se encuentran bajo el dominio de la Entidad, que afecten directamente los servicios prestados (orden público, vandalismo, etc.).

También se deben considerar la identificación de factores desencadenantes, tales como los cambios en el contexto y cambios en los niveles de riesgo que puedan generar nuevamente la valoración de los riesgos o generen alertas tempranas sobre los cambios en el apetito por riesgo.

En caso de identificar nuevos factores de riesgo que interfiera con la caracterización del riesgo, es necesario evaluar y documentar su pertinencia y realizar la respectiva solicitud al Grupo de Resiliencia Operacional para ser incluido en las herramientas de gestión de riesgos para el uso de toda la Entidad.

6.3.2.5 Clasificación del riesgo

Una vez identificado el riesgo y definida la descripción de este, se debe seleccionar el factor al cual se identificó teniendo en cuenta las fuentes generadoras del mismo y definir el tipo de riesgo al que hace referencia.

Los tipos de riesgos identificados en la Entidad son:

- **Riesgo de Ciberseguridad:** Son los riesgos que se relacionan con las pérdidas que se originan por la afectación en los activos de la Entidad, que se encuentran en el ciberespacio.

[8] El detalle de las variables asociadas a cada factor de riesgo se encuentra en la proforma interna E-PI-PLA-018- hoja “FACTORES DE RIESGO”.

- **Riesgo de Continuidad:** Comprende los riesgos que afectan la operación normal de la Entidad dada la indisponibilidad de los servicios, que ocasionen la interrupción en la entrega de un producto.

- **Riesgo de Corrupción:** Es la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

- **Riesgo de Cumplimiento:** Son los riesgos relacionados con la capacidad de la Entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad debido a su incumplimiento o desacato a la normatividad legal y/o las obligaciones contractuales.

- **Riesgo Estratégico:** Se asocia a los riesgos que afectan la misión y/o el cumplimiento de los objetivos estratégicos de la Entidad, debido a la inadecuada definición de políticas, diseño y conceptualización de la Entidad por parte de la Alta Dirección. Eventos que afecten los objetivos estratégicos de la organización pública y por tanto impactan toda la Entidad.

- **Riesgo de Lavado de Activos, Financiación del Terrorismo y la Financiación de la Proliferación de Armas de Destrucción Masiva (LA/FT/FPADM):** Se relaciona con la posibilidad de afectación o daño a la Entidad por ser utilizada como instrumento para la realización de operaciones de lavado de activos y/o canalización de recursos hacia la realización de actividades ilícitas.

- **Riesgo Operativo:** Corresponde al riesgo de falla en la operación derivado de la inadecuación o errores en los procesos internos, del personal, de los sistemas y de los controles internos aplicables o bien a causa de acontecimientos externos. Nota**:** Los riesgos relacionados con el Hardware (equipos y plataforma tecnológica) y Software de la Entidad se encuentran clasificados en el riesgo operativo.

- **Riesgo de Proyectos de Inversión:** Corresponde a los riesgos que pueden llegar a afectar los objetivos de un proyecto de inversión durante el horizonte de ejecución de este. Los riesgos de este tipo se encuentran registrados en la Metodología General Ajustada – MGA. Este tipo de riesgos debe incorporarse en los procesos aplicables.

- **Riesgo de Seguridad digital:** Comprende los riesgos que afectan alguno de los principios de la seguridad digital: Confidencialidad, Integridad y disponibilidad de la información. Incluye aspectos relacionados con el ambiente físico, digital y las personas. Combinación de amenazas y vulnerabilidades en el entorno digital.

6.4 VALORACIÓN DEL RIESGO

La valoración del riesgo inicia con la definición de la probabilidad de ocurrencia y el nivel de impacto de acuerdo con análisis del proceso y los criterios definidos, para

conocer la zona en donde se encuentra el riesgo en el momento inicial (o conocido como Riesgo inherente) y determinar la zona de riesgo final luego de implementar los controles (conocida como Riesgo Residual).

Es responsabilidad de los procesos contemplar el resultado del análisis de contexto interno y externo, así como el grado de afectación en las partes interesadas durante el ejercicio de valoración de los riesgos.

Se recomienda utilizar algunos aspectos relevantes para la valoración del riesgo, como son:

- El valor de la información del proceso para la Entidad.
- La criticidad de los activos de información involucrados en el proceso.
- Los requisitos legales y reglamentarios, así como las obligaciones contractuales.
- La repercusión en el medio ambiente
- La importancia de la disponibilidad, de la confidencialidad, y la integridad de la información para las operaciones y la Entidad.
- Las expectativas, necesidades y percepciones de las partes interesadas.

6.4.1 Análisis del riesgo

En esta etapa se define la probabilidad de ocurrencia y el impacto de los riesgos a los que se ve expuesto el proceso, sin tener en cuenta el efecto que generan los controles en su mitigación (riesgo inherente).

Probabilidad: La variable probabilidad de ocurrencia se define con base en el número de veces en que se pasa por el punto de riesgo (actividad originadora del riesgo) en un período de un año.

La probabilidad de ocurrencia del riesgo se analiza según la ***frecuencia*** con la cual se realiza la actividad que puede originar el riesgo, por lo tanto, es importante tomar como referencia la caracterización de cada proceso objeto de análisis. Por ejemplo, para un riesgo relacionado con la publicación semestral de un documento, la frecuencia seria 2 veces al año.

Nota: Cuando el factor de riesgos sea tecnológico, la frecuencia debe ser medida en horas, 1 hora funcionamiento = 1 vez. Por ejemplo, un riesgo relacionado con afectación a la confidencialidad de la información almacenada en activos cibernéticos, la cual está expuesta a ser atacada los 365 días al año las 24 horas, su frecuencia será 365 x 24 =8.760 veces al año.

En el campo “Probabilidad/Frecuencia Inherente”, en la Hoja C. RIESGOS (E-PI-PLA-018), se describirá la frecuencia de la actividad originado del riesgos durante un periodo anual. De acuerdo con esta información, la proforma determina el nivel de probabilidad de ocurrencia, según la siguiente tabla:

Tabla 1. Cálculo de la probabilidad

Tabla de Probabilidad			
Nivel	**Nivel**	**Frecuencia de la actividad**	**Probabilidad**
5	**Muy Alta**	La actividad que conlleva el riesgo se realiza más de 5000 veces al año.	100%
4	**Alta**	La actividad que conlleva el riesgo se realiza de 501 a 5000 veces al año.	80%
3	**Media**	La actividad que conlleva el riesgo se realiza de 25 a 500 veces por año.	60%
2	**Baja**	La actividad que conlleva el riesgo se realiza de 3 a 24 veces al año.	40%
1	**Muy Baja**	La actividad que conlleva el riesgo se realiza máximo 2 veces por año.	20%

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - DAFP

Impacto: Corresponde a la magnitud de la pérdida para la Entidad dado los efectos que tiene la materialización de un riesgo. Se mide desde dos dimensiones: la económica y la reputacional.

La valoración del impacto se realiza de manera independiente para cada riesgo teniendo en cuenta la descripción consignada en la tabla de impacto relacionada a continuación:

Tabla 2. Cálculo del Impacto

Tabla de Impacto			
Niveles	**Impacto**	**Afectación económica**	**Reputacional**
5	**Catastrófico**	Mayor a 500 SMLMV	El riesgo afecta la imagen de la Entidad a nivel nacional, con efecto publicitario sostenido a nivel país
4	**Mayor**	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la Entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
3	**Moderado**	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la Entidad con algunos usuarios de relevancia frente al logro de los objetivos.
2	**Menor**	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la Entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
1	**Leve**	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la organización.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - DAFP

Puede existir riesgos que generen afectación económica y reputacional, para estos casos, se toma el impacto que tenga mayor peso en la valoración, es decir, si el impacto económico es “Moderado” y el impacto reputacional es “Mayor”, predomina la valoración del impacto reputacional debido a que es la que tiene una mayor valoración. Si la afectación económica y reputacional tienen la misma valoración, se debe seleccionar la opción “Económica y Reputacional” en el campo “Tipo de Impacto" de la hoja C. RIESGOS en la proforma interna.

El resultado de la etapa de análisis de riesgos busca que la Entidad obtenga información suficiente para:

- Establecer la probabilidad de ocurrencia de los riesgos, que pueden disminuir la capacidad institucional, para cumplir su propósito o misión.
- Medir el impacto, las consecuencias del riesgo sobre las personas, los recursos o la coordinación de las acciones necesarias para el logro de los objetivos institucionales o el desarrollo de los procesos.
- Establecer criterios de calificación y evaluación de los riesgos que permiten tomar decisiones pertinentes sobre su tratamiento.

No obstante, con el fin de realizar un análisis integral del riesgo, y teniendo en cuenta la tipología definitiva previamente para el mismo, es necesario considerar otros factores diferentes a la probabilidad e impacto, tales como la complejidad, la interconexión, la temporalidad, la volatilidad, la sensibilidad, el nivel de confianza, entre otros.

6.4.2 Evaluación del riesgo

La evaluación del riesgo consiste en determinar los niveles de riesgo inicial (riesgo inherente) y final (riesgo residual), de acuerdo con las variables definidas anteriormente y los controles que el proceso establezca para su mitigación.

6.4.2.1 Riesgo Inherente

La fase de evaluación del riesgo inicia con la determinación de la zona de riesgo inicial (o RIESGO INHERENTE), a través de la combinación entre las variables probabilidad de ocurrencia e impacto, definidas en la fase de análisis del riesgo, las cuales, de acuerdo con el mapa de calor y los niveles de riesgo definidos por la Entidad, establecen la criticidad de este[9].

Los niveles de riesgos definidos, según la severidad de este, en la Entidad son:

Tabla 3 Nivel del riesgo

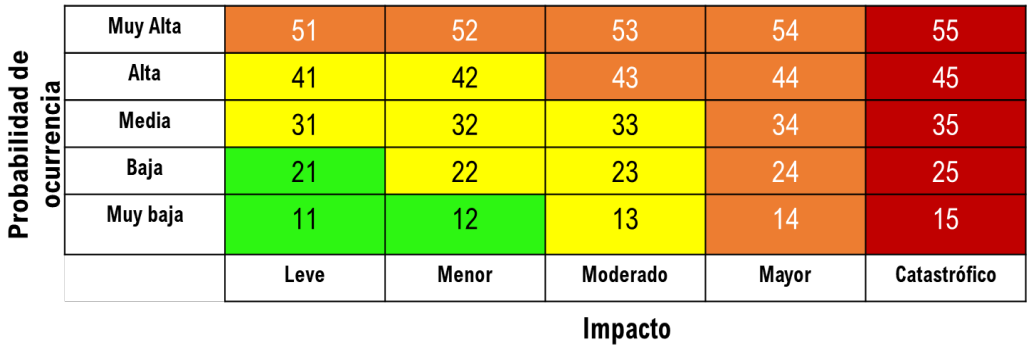
[9] El riesgo inherente y el cuadrante en el mapa de calor en donde se ubica el riesgo inicialmente, se generan de manera automática en la proforma interna E-PI-PLA-018, en la hoja C.RIESGOS, una vez definidas las variables probabilidad de ocurrencia e impacto.

Nivel de Riesgo	
Bajo	
Moderado	
Alto	
Extremo	

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas – DAFP

Los cuadrantes del mapa de calor, según la combinación de las variables probabilidad de ocurrencia e impacto son[10]:

Imagen 1. Mapa de calor de riesgos



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas – DAFP (ajustado por la Entidad)

6.4.2.2 Identificación de Causas

Una vez se tiene el resultado del riesgo inherente, se debe detallar las causas, medios, circunstancias, hechos y/o razones que puedan generar la materialización del riesgo.

Para definir las causas de los riesgos se puede considerar lo siguiente:

- El análisis del contexto interno y externo y la Matriz DOFA por proceso

[10] El primer carácter del número de cuadrante indica el nivel de probabilidad en la escala de 1 a 5 y el segundo carácter el impacto.

- Los objetivos estratégicos y de proceso, los cuales se desarrollan a través de actividades, pero no todas contribuyen en el mismo grado para lograr los objetivos del proceso.
- Las actividades críticas o factores claves de éxito, dado que son las que aportan en forma significativa al logro de los objetivos; estos factores constituyen elementos para identificar las causas o factores que originan la materialización de los riesgos.

A manera de ejemplo se enumeran las siguientes circunstancias como causas de un riesgo:

- Errores u omisiones en la ejecución de los requisitos establecidos.
- Falta de políticas
- Falta de competencia de los agentes generadores
- Deficiente selección de personal
- Falta de competencia de los funcionarios
- Falta o deficiencia en los filtros para la toma de decisiones.
- Carencia de controles.
- Deficiencia en la comunicación entre procesos
- Necesidad del desarrollo de actividades presenciales
- Dependencia de documentos físicos
- Fallas en acceso remoto
- Contagios/pandemia
- Incumplimiento contractual
- Fallas en la cadena de suministros
- Indisponibilidad de proveedores
- Afectación al presupuesto
- Ciberataque
- Interrupciones no planeadas en servicios de tecnología
- Interrupción del suministro de energía
- Incidentes de seguridad.
- Eventos climáticos extremos
- Desastres naturales

Para la codificación de las causas, estas deben iniciar con la sigla “CAU”, seguido del consecutivo de cada una de estas. Ejemplo: CAU_001, CAU_115, etc.

Las causas identificadas pueden aplicar a diferentes riesgos, dentro de la misma matriz, por lo tanto, es importante considerar que no se debe cambiar el código de la causa en cada riesgo, es decir, se mantiene el mismo código de causa independiente del riesgo que se esté manejando.

6.4.2.3 Controles

La Superintendencia Financiera de Colombia cuenta con un sistema de administración y gestión de controles para el control de las amenazas inherentes al desarrollo de su actividad, en el cual se identifican, miden y se monitorean las actividades de control.

Las actividades de control son entendidas como las acciones detectivas y preventivas oportunas para evitar la materialización del riesgo y/o la actuación correctiva inmediata ante las eventualidades para mitigar las posibles consecuencias a fin de mantener los niveles de riesgo aceptables.

Le corresponde a la primera línea de defensa (líderes de proceso) el establecimiento de actividades de control, a través de políticas y/o procedimientos. Las actividades de control se orientan para prevenir, detectar y corregir la materialización de los riesgos. Por consiguiente, su efectividad deriva en el logro de los objetivos estratégicos y del proceso.

Para la definición de controles es importante, considerar:

- Debe existir al menos un control por cada causa identificada.
- No es válido definir el mismo control para dos o más causas diferentes dentro de un mismo riesgo, debido a que se puede presentar alteraciones en la valoración del riesgo residual. En caso de que un control aplique para diferentes causas, se debe unificar las causas en una misma celda.
- Una política por sí sola no es un control, siempre es necesario describir el control con la estructura definida, la cual implica describir una acción.
- Los controles se precisan a través de los procedimientos del proceso (hacen parte del día a día de los procesos).
- Los controles deben contemplar en su descripción palabras tales como revisar, verificar, cotejar, validar, realizar seguimiento, comprobar, confrontar o evidenciar entre otras que contribuya a confirmar la ejecución y validez de una tarea.
- Para adelantar esta etapa, se hace necesario tener claridad sobre los puntos de control existentes en los diferentes procesos, los cuales permiten obtener información para efectos de toma de decisiones.

Para la descripción del control se debe considerar todos los detalles que sean necesarios para que sea de fácil entendimiento a personas ajenas al proceso. La estructura que se debe seguir para su redacción es la siguiente: Responsable de la Ejecución del Control + Acción + Complemento.

Responsable de la Ejecución del Control: Es el funcionario o persona responsable de ejecutar el control. Se debe relacionar el cargo del responsable. Para los controles de tipo de implementación automática, se debe relacionar el sistema y/o aplicativo que ejecuta la actividad.

Acción: Corresponde a la actividad a desarrollar con el objetivo de prevenir, detectar o corregir la materialización del riesgo. Se debe definir con un verbo que indique la acción que deben realizar como parte del control. Adicionalmente, el control debe tener un propósito que indique para qué se realiza, y debe ser coherente con la causa que busca atacar.

Complemento: Corresponde a los detalles adiciónales que permitan identificar claramente el objeto del control, para cualquier persona que lo lea. El complemento del control debe indicar, al menos:

- La periodicidad en la que se ejecuta el control.
- La forma como se realiza el control, de tal manera que se pueda evaluar si la fuente u origen de la información que sirve para ejecutar el control es confiable para la mitigación del riesgo.
- Como es el tratamiento de las observaciones o desviaciones como resultado de ejecutar el control, con el fin de conocer el paso a seguir.
- La evidencia de la ejecución del control, con el fin de conocer los resultados del control. Hay controles en los que su evidencia queda en un flujo a través de una aplicación como un "aprobado" o "revisado" y otros en los que la evidencia es la configuración y programación de la aplicación, cuando es un control automático.
- El nombre de la referencia documental (procedimiento, política, manual, instructivo o guía) con el código de referencia en el SGI, en donde se encuentra documentado el control.

Ejemplo:

Responsable	Acción	Complemento
El profesional de Talento Humano encargo de la vinculación de funcionarios	Verifica que la información suministrada por los futuros funcionarios cumpla con los lineamientos de contratación establecidos por la Entidad	A través de la lista de chequeo de requisitos de información e inhabilidades. En caso de cumplir con todos los requisitos, procede a cargar la información en el sistema para continuar con el tramite de contratación. Como evidencia se cuenta con el check list, adjunto en la carpeta de cada servidor. El control se encuentra documentado en el procedimiento A-GU-GTH-004.

La administración de los controles, está a cargo del Grupo de Resiliencia Operacional y se realiza a través del inventario de controles definido en la proforma interna E-PI-PLA-018, en la hoja INVENTARIO CONTROLES. Este consolida y homologa los controles registrados en las matrices de riesgos de los 21 procesos, con el fin de unificar la descripción y atributos de estos y realizar un adecuado seguimiento.

El administrador del inventario asignara un código único a cada control, el cual inicia con la sigla "CTRL" seguida de un consecutivo de 3 dígitos. Ejemplo: CTRL_001, CTRL_414.

Teniendo en cuenta que dicho inventario solo podrá ser modificado por el Grupo de Resiliencia Operacional, es necesario enviar las solicitudes o novedades (adicionar nuevos controles, eliminar controles que ya no estén funcionando, modificar la descripción o los atributos de los controles, etc.) que se requieran sobre el mismo al correo resiliencia.operacional@superfinanciera.gov.co, con el fin de evaluar y realizar

los ajustes necesarios. El Grupo de Resiliencia Operacional contará con un tiempo de cinco (5) días hábiles para responder a dicha solicitud.

Para la inclusión de nuevos controles se debe enviar la propuesta al correo mencionado anteriormente, indicando a que riesgo y causa está destinada su mitigación y será el Grupo de Resiliencia Operacional quien realice las pruebas de escritorio sobre el diseño, eficiencia y pertinencia de este. Una vez el control cumpla satisfactoriamente con todos los criterios definidos en las pruebas realizadas, el Grupo de Resiliencia Operacional procederá a actualizar el inventario de controles.

Cuando se solicite realizar la eliminación del control, este será inactivado en el inventario de controles, en la columna "Estado" y por lo tanto, no genera ninguna eficiencia sobre el control.

Los lideres de proceso deben seleccionar en el campo "Código Control", de la hoja C. RIESGOS el número de control que mitigue el riesgo en gestión, según el inventario de controles. La proforma traerá automáticamente la descripción y los atributos del control. Para facilitar la búsqueda, se propone identificar los controles según el tipo y/o factor de riesgo.

El Grupo de Resiliencia Operacional apoyará a los procesos en evaluar la factibilidad de diseñar los planes de contingencia, de continuidad y los controles de tipo técnico para la implementación por parte de la Dirección de Tecnologías de la Información (software o hardware). Por lo anterior, si es viable definir y desarrollar un plan de contingencia o controles técnicos se debe elaborar el plan de acción o de mejora en el aplicativo del SGI.

Atributos de Eficiencia del Control

La eficiencia de un control es entendida como la medición de las acciones tomadas, a través de la definición del grado de aporte que genera para la mitigación del riesgo. La Entidad considera dos clases de atributos para medir la eficiencia del control:

a. Tipo de control

- **Preventivo:** Aquellos controles que actúan para eliminar las causas que originan el riesgo, para prevenir su ocurrencia o su materialización (evita un evento no deseado). Se basa en prevenir posibles problemas posteriores en el desarrollo de las actividades cotidianas, por lo tanto, se ejecutan en las entradas del proceso. Este tipo de control disminuye la variable probabilidad de ocurrencia. Ejemplo: Revisiones, mantenimientos, etc.
- **Detectivo:** Controles que están diseñados para identificar las fallas en la entrega de productos y/o servicios del proceso ante un resultado no previsto. Buscan detectar la situación no deseada para que se corrija y se tomen las acciones correspondientes y evitar la materialización del riesgo, por lo tanto, mitigan la variable probabilidad de ocurrencia. Ejemplo: Realizar conciliaciones bancarias, verificación de cumplimiento de requisitos, etc.

- **Correctivo**: Son controles que se diseñan para mitigar los efectos o consecuencias de la materialización de un evento de riesgo, por lo tanto, disminuyen la variable impacto. Ejemplo: Activación de los planes de contingencia, reportes a entes de control, etc.

b. Tipo de implementación

- **Manual:** Actividades diseñadas para ser ejecutadas por una persona, por lo cual se puede generar un error humano.
- **Automático:** Son actividades de procesamiento o validación de información que se ejecutan por un aplicativo de manera automática sin la intervención de personas para su realización.

Atributos Informativos del Control

La definición de los atributos informativos de los controles, permiten indicar la formalidad del control a través de características cualitativas que establecen si el control existe y está en ejecución o es un control nuevo que se va implementar. Por lo anterior, estos atributos no tienen incidencia sobre la eficiencia en la mitigación del riesgo.

a. Documentación

- **Documentado:** Hace referencia a los controles que están documentados en los procedimientos, manuales, flujogramas o cualquier otro documento propio de la Entidad.
- **Sin Documentar:** Hace referencia a los controles que pese a que se ejecutan con la periodicidad indicada, no se encuentran documentados en ningún documento de la Entidad.

b. Frecuencia

- **Continua:** Se refiere a los controles que se ejecutan con la misma periodicidad con la que se realiza la actividad originadora del riesgo. Tiene una periodicidad definida.
- **Aleatoria:** Se refiere a los controles que no se ejecutan con una periodicidad definida.

c. Evidencia

- **Con Registro:** Hace referencia a los controles que cuentan con evidencia de la ejecución de este. Ejemplo: correos electrónicos, cartas con firma mecánica, firmas digitales, actas de Comités, firma de asistencia a capacitaciones, entre otros.
- **Sin Registro:** Hacen referencia a los controles que se ejecutan, pero al validar algún tipo de evidencia de su ejecución no es posible determinarla.

La evaluación de los controles define el nivel de eficiencia en la mitigación del riesgo, la cual se realiza de manera acumulativa, tomando como referencia el resultado de la medición del control inmediatamente anterior, según los pesos definidos en la siguiente tabla:

Tabla 4. Tabla de valoración de controles

Características			Peso
Atributos de Eficiencia	Tipo	Preventivo	25%
		Detectivo	15%
		Correctivo	10%
	Implementación	Automático	25%
		Manual	15%
Atributos Informativos	Documentación	Documentado	-
		Sin Documentar	-
	Frecuencia	Continua	-
		Aleatoria	-
	Evidencia	Con Registro	-
		Sin registro	-

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - DAFP

6.4.2.4 Riesgo Residual

El resultado de la eficiencia de los controles definidos en la fase de evaluación define el riesgo residual o zona final y el cuadrante en el mapa de calor en el cual se ubica, para establecer el nivel de riesgo final sobre el cual se priorizarán las acciones para la mitigación de este.[11]

6.4.3 Tratamiento del riesgo residual

En esta fase se definen las estrategias para tratar los riesgos residuales que se encuentren por fuera del apetito por riesgo de la Entidad, con el fin de mitigar la ocurrencia y/o el impacto de la materialización de estos.

Las estrategias para combatir el riesgo se enmarcan en las siguientes categorías:

- **Transferir el riesgo:** Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los dos principales métodos de compartir o transferir parte del riesgo son: seguros y tercerización. Estos mecanismos de transferencia de riesgos deberían estar formalizados a través de un acuerdo contractual.

[11] El riesgo residual y el cuadrante en el mapa de calor en donde se ubica el riesgo final, se generan de manera automática en la proforma interna E-PI-PLA-018, en la hoja C.RIESGOS, una vez definidas las causas y controles del riesgo.

- **Reducir o mitigar el riesgo:** Se mitiga la ocurrencia y/o el impacto del riesgo a través de un plan de acción con actividades diferentes a las definidas en los controles.

- **Aceptar el riesgo**: No se implementan medidas que afecte la probabilidad o el impacto del riesgo, asumiendo las consecuencias de la materialización de este.

- **Evitar el riesgo:** Cuando el nivel de riesgo es muy alto, se puede definir abandonar las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.

A la hora de evaluar las opciones existentes en materia de tratamiento del riesgo, los líderes de procesos deberán tener en cuenta el impacto que tiene el riesgo sobre la Entidad y sus partes interesadas, la probabilidad de ocurrencia, el nivel de impacto y la relación costo-beneficio del tratamiento.

Los procesos deben iniciar el tratamiento de los riesgos con la opción de reducir o mitigar el riesgo, buscando implementar nuevos controles y/o realizando actividades de tipo interno. Estas actividades deben establecerse a través de un plan, programa o acción de mejora en el que se defina un responsable, fechas de implementación y de seguimiento y entregables, formalizado en el SGI[12].

Posteriormente, y dados los resultados del plan de acción inicial, el proceso podrá gestionar actividades para compartir, aceptar o evitar el riesgo.

Cuando se evidencie que una de las causas del riesgo es derivada de la deficiencia en el conocimiento de los vinculados que ejecutan las actividades del proceso, se deberán definir y gestionar actividades de capacitación y/o sensibilización.

6.4.3.1 Criterios para la Priorización de Riesgos

Priorizar la gestión de los riesgos permite identificar aquellos que representan una mayor amenaza para el logro de los objetivos, para responder ante ellos en primer lugar, con los recursos de los que dispone la Entidad.

Para identificar los riesgos sobre los que debe primar el tratamiento y/o la gestión, es importante considerar los siguientes criterios:

- En primer lugar, se debe priorizar por el nivel de riesgo, es decir, según su gravedad. Los procesos deberán establecer acciones que busquen mitigar la materialización de riesgos que se encuentren en niveles iguales o superiores a "Moderado".
- Adicionalmente, se debe prestar atención y enfocar esfuerzos en aquellos riesgos que presenten un nivel de la variable impacto residual Mayor o Catastrófico, con el

[12] El plan de acción definido para el tratamiento de los riesgos, deberá registrase en la hoja “E. TRATAMIENTO RIESGOS”, en la proforma interna E-PI-PLA-018, en el campo “Plan de Acción”.

fin de definir planes de respuesta que busquen neutralizar el impacto en caso de materializarse el riesgo.

- En tercer lugar, se deberán identificar los riesgos que presenten un nivel de probabilidad de ocurrencia residual Alta y Muy Alta, con el propósito de establecer actividades de tratamiento para evitar la materialización del riesgo.
- Finalmente, se debe considerar la capacitad de gestión del riesgo, lo que implica establecer diferentes opciones de respuesta para aquellos riesgos que se consideran urgentes dado que se espera que su ocurrencia se presente en el corto plazo.

6.5 SEGUIMIENTO Y MONITOREO

Con el objetivo de realizar el monitoreo de los riesgos asociados a los procesos, la Oficina Asesora de Planeación realiza actividades de seguimiento continuo sobre las novedades en riesgos que permiten tomar acciones tempranas en pro de realizar una adecuada gestión de riesgos. Adicionalmente, se deberán realizar tres seguimientos periódicos de la siguiente manera:

6.5.1 Seguimiento Mensual

Se realiza con el fin de verificar el cumplimento de las actividades propuestas para el tratamiento de riesgos y el fortalecimiento de los controles e identificar las materializaciones de riesgos registradas durante el mes. Así mismo, se debe indicar si durante el mes de análisis se presentan novedades en las matrices de riesgos de los procesos.

Este reporte está a cargo de los Coordinadores de Calidad, quienes deberán enviar vía correo electrónico dicha información al Grupo de Resiliencia Operacional, durante los primeros diez (10) días calendarios seguidos al corte de mes (en caso de coincidir con fin de semana o festivo se correrá la fecha para el siguiente día hábil).

Una vez recibida la información por el Grupo de Resiliencia Operacional, se consolida y se verifica. En caso de no contar con información clara, se enviará un correo solicitando las aclaraciones y/o ajustes correspondientes.

El resultado del seguimiento se presenta en los diferentes comités institucionales que se agenden durante el mes siguiente al corte.

6.5.2 Seguimiento Trimestral

Este seguimiento es realizado por los Líderes y Facilitadores de los procesos, con el propósito de identificar novedades frente a los riesgos y controles registrados en las matrices de riesgos, así como el avance en las estrategias DOFA y los planes de acción para el tratamiento de los riesgos y el fortalecimiento de controles.

Dicho reporte se realiza a través de la opción “Reportes y solicitudes al SGI”, en el cual se deberá adjuntar las hojas “B. ESTRATEGIAS DOFA” y “E. TRATAMIENTO

RIESGO" de la proforma interna, con el avance en las actividades propuestas por el proceso. Así mismo, deberá adjuntar o referenciar la ruta en donde se encuentran las evidencias de estas.

El proceso deberá indicar en la hoja "E. TRATAMIENTO", en el campo "Seguimiento/Observaciones", mínimo:

- El seguimiento y/o avance en el plan de acción para el tratamiento de los riesgos y/o el fortalecimiento de controles.
- Reportar la materialización de los riesgos vigentes en la matriz, durante el trimestre.
- Reportar las novedades que surjan en la evaluación de la continuidad de los riesgos identificados en la matriz de riesgos del proceso, así como la evaluación inicial de las variables probabilidad de ocurrencia e impacto, por parte del proceso.
- Reportar las novedades que se generen del seguimiento a la pertinencia y continuidad de los controles definidos para la mitigación de los riesgos realizado por el proceso.
- Reportar la identificación de nuevos riesgos y/o controles para el proceso, con el fin de realizar un acompañamiento en la actualización de la matriz de riesgos, por parte del Grupo de Resiliencia Operacional.

Si al momento de recibir el reporte no se identificas novedades, frente a los riesgos y controles registrados en las matrices de riesgos, se dará por entendido que estos se mantienen y siguen siendo aplicables al proceso.

El reporte de seguimiento se debe realizar con corte a los meses de marzo, junio, septiembre y diciembre. Los líderes y/o facilitadores de proceso cuentan con 15 días calendario después de la fecha de corte, para el envío del reporte. En caso de coincidir con fin de semana o festivo se correrá la fecha para el siguiente día hábil.

Por su parte, una vez finalizada la fecha máxima de reporte por parte de los procesos, el Grupo de Resiliencia Operacional contará con cinco (5) días hábiles para consolidar, analizar y reportar la información enviada por parte de los procesos.
Dicha información es fuente principal para realizar la actualización del perfil de riesgos de la Entidad, los mapas de riesgos, el inventario de controles y la definición de riesgos de primer nivel.

El informe del seguimiento se presenta en los diferentes comités institucionales, según la periodicidad definida para cada uno de estos. Los costos de estos se miden en el tiempo que deben invertir los encargados de generar dichos informes y las herramientas tecnológicas que debe disponer para que la información que llegue a la Alta Dirección sea clara y permita tomar decisiones acertadas en lo referente a la gestión de riesgos.

6.5.3 Seguimiento Anual

Corresponde a los Lideres y Facilitadores de los procesos, con apoyo de los Coordinadores de Calidad y el Grupo de Resiliencia Operacional, evaluar al menos una vez por año la matriz de riesgos de su proceso.

Para tal fin, el proceso deberá considerar la última actualización a la metodología de riesgos y el cronograma de actividades establecido por el Grupo de Resiliencia Operacional para el desarrollo de la actualización de las matrices en toda la Entidad, durante el primer semestre del año.

En este seguimiento, los procesos deben considerar e implementar todos los aspectos de la presente metodología desde su fase previa de análisis de contexto hasta su fase final de información y consulta. El resultado de dicha implementación debe ser enviado al Grupo de Resiliencia Operacional, para su respectiva revisión y solicitud de ajustes, previo a la oficialización de la matriz de riesgos en el aplicativo SGI.

El Grupo de Resiliencia Operacional es el encargo de consolidar la información y generar los informes de resultado del análisis de esta, con el fin de obtener el estado actual de los riesgos para definir, revaluar o mantener el perfil de riesgo, el apetito por riesgo, los mapas de riesgos, el inventario de controles, los riesgos de primer nivel y el tratamiento de riesgos.

El informe final del presente seguimiento es presentado en los diferentes comités institucionales en los que el Grupo de Resiliencia Operacional participe, con el fin de ratificar o modificar los niveles para la gestión de riesgos.

6.6 INFORMACIÓN Y CONSULTA

El proceso de comunicación de la gestión de riesgos debe consideran un alcance hacia todos los funcionarios de la Entidad, promoviendo el aprendizaje continuo, la innovación y el trabajo en equipo, para apoyar el cumplimiento de los objetivos estratégicos de la organización.

Es importante asegurarse de que exista una cultura organizacional de riesgos, en donde todos los funcionarios comprendan, de acuerdo con su papel en la Entidad, cuál es la estrategia de riesgo, prioridades, metodologías, tratamientos, herramientas y responsabilidades frente a la gestión de este.

Para asegurar la correcta comunicación hacia las partes interesadas en la gestión de riesgos, se asigna a la Oficina Asesora de Planeación y al Grupo de Resiliencia Operacional, la función de reportar ante el Comité Institucional de Gestión y Desempeño y al Comité institucional de Coordinación de Control Interno, la idoneidad y eficacia de los controles, el seguimiento de los tratamientos, la identificación y valoración de nuevos riesgos y cualquier otro aspecto que se considere relevante informar para la toma de decisiones.

6.6.1 Canales de Comunicación para el Reporte de Situaciones de Riesgo

La comunicación del riesgo se refiere al intercambio de información sobre las amenazas que enfrenta la Entidad, tanto por parte del Grupo de Resiliencia (divulga información) como por parte de cualquier funcionario que detecte una situación que amenace a la Entidad (reporta EVIAs).

Es responsabilidad de cualquier funcionario que detecte una amenaza reportar a la segunda línea de defensa la presencia del hecho.

Los medios de comunicación definidos para el reporte y divulgación de situaciones de riesgos en la Entidad son:

- Correo de resiliencia.operacional@superfinanciera.gov.co para el reporte de EVIAs (Eventos, Vulnerabilidades, Incidentes, Alertas).
- Aplicativo ISOLUCION, por la opción “Reportes y Solicitudes al SGI”, para el registro y reporte de los eventos de riesgo.
- Boletines Yammer, para la divulgación de información sobre la gestión de riesgos por parte de la segunda línea de defensa (OAP-Grupo de Resiliencia Operacional).

6.6.2 Reporte de Eventos de Riesgos y/o Materialización de riesgos

Un evento de riesgo es la ocurrencia de una situación adversa, generada por un factor de riesgo, que genera un impacto para la Entidad y que tiene la capacidad de alterar el curso normal de las actividades. Ocurre en un lugar particular en un intervalo de tiempo determinado y puedo o no generar una pérdida.

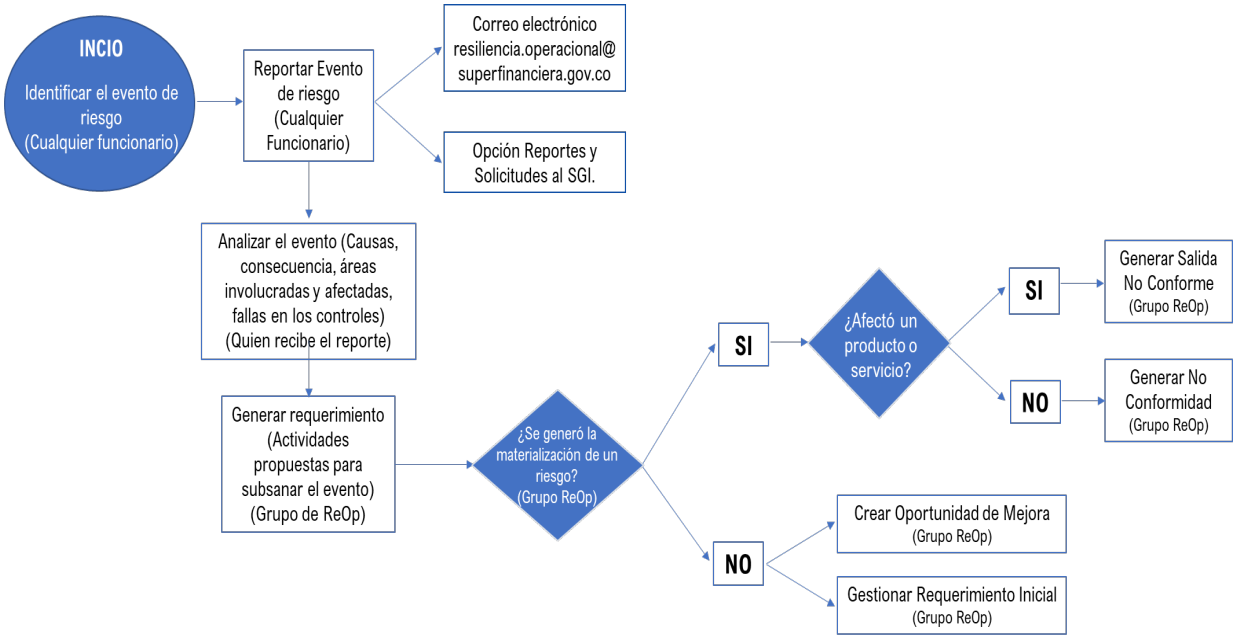
La materialización del riesgo se refiere a la generación de una pérdida para la Entidad (ya se económica o reputacional) a causa de la presencia de un evento de riesgo.

Para el reporte del evento de riesgo, se debe relacionar lo siguiente:

- **Evento –** Qué sucedió.
- **Sitio –** Área o dependencia
- **Cómo sucedió –** Describir la forma cómo ocurrió el evento teniendo en cuenta la actividad del proceso que se estaba realizando.
- **Tiempo –** Cuándo sucedió
- **Efectos** o consecuencias que generó.

El reporte de los eventos de riesgos y/o sus materializaciones, se realiza siguiendo el procedimiento de EVIAs definido en la Guía de Definición de EVIAE-GU-PLA-024 y sigue el siguiente flujo para su respectiva gestión:

Imagen 2. Flujo para la gestión de eventos de riesgos



Una vez se genera el registro, el Grupo de Resiliencia Operacional analizará el evento y definirá la acción de mejoramiento (requerimiento, oportunidad de mejora, salida no conforme o no conformidad) a definir para la remediación de este. A partir de la definición del plan, el Líder del Proceso dispondrá de 3 días hábiles para aprobar o rechazar este. En caso de ser aceptada, para el caso de las Oportunidades de Mejora, la No Conformidad o la Salida No Conforme, el proceso contara con 8 días hábiles para la definición de la corrección y el plan de acción correspondiente.

En caso de rechazar la materialización del riesgo, el Líder del proceso enviará correo electrónico a resiliencia.Operacional@superfinanciera.gov.co informando la causa de dicha acción. El Grupo de Resiliencia Operacional, en un máximo de 3 días, evaluará la justificación dada y decidirá si da por finalizado el reporte o si procede con la creación de la acción correctiva al proceso correspondiente.

Nota: Cuando el Grupo de Resiliencia Operacional identifique o sea notificado de un evento que genere afectación frente a la confianza, disponibilidad o integridad de la información almacenada en activos cibernéticos, procederá a realizar el análisis correspondiente con el fin de determinar las causas y consecuencias para establecer acciones que mitiguen la ocurrencia y el impacto del riesgo.

7. HERRAMIENTAS PARA LA GESTIÓN DEL RIESGO

La Superintendencia Financiera de Colombia cuenta con las siguientes herramientas que contribuyen con la identificación, evaluación y tratamiento de los diferentes tipos de riesgos en la Entidad:

- Mapas de riesgos (Interno/Externo)
- Histórico de riesgos materializados
- Indicadores de gestión por proceso y subproceso
- Matriz DOFA por proceso
- Planes de mejoramiento en el SGI
- Riesgos de primer nivel

7.1 Planes de mejora para la gestión del riesgo en el SGI

Una vez surtida todas las fases definidas en la metodología de riesgos presente, los procesos deberán identificar la necesidad y/o obligatoriedad de crear planes de mejoramiento para la gestión del riesgo, especialmente, de aquellos que se encuentren por fuera del apetito por riesgo de la Entidad.

Los procesos deberán crear oportunidad de mejora en el aplicativo SGI, cuando:

i) Existan riesgos que se encuentren por fuera del apetito por riesgo de la Entidad, dado que requieren implementar actividades de tratamiento del riesgo.
ii) Existan controles que no se encuentren documentados, con el fin de establecer actividades para su formalización.
iii) Existan controles que no generen evidencia de su ejecución, con el fin de establecer actividades para definir el registro del control.
iv) Las actividades definidas en las estrategias DOFA no se encuentren asociadas en un plan, programa o proyecto, con el propósito de realizar un seguimiento sobre estas.

Nota: Cuando los riesgos residuales que se encuentren por fuera del apetito por riesgo sean solo de tipo “Riesgo de Corrupción”, no es necesario crear oportunidad de mejora, dado que el tratamiento de estos riesgos está a cargo del Grupo para la Transparencia y Lucha Contra la Corrupción. Es potestad de los procesos crear la oportunidad de mejora para establecer actividades a nivel interno para el tratamiento de estos riesgos.

Las actividades definidas en el plan de acción deberán contener el responsable o líder del desarrollo, la fecha final de ejecución y el entregable de dicha actividad y se deberán relacionar en la hoja “E: TRATAMIENTO RIESGOS”, de la proforma interna, previo a la oficialización de la matriz de riesgos en el SGI.

7.2 Riesgos de primer nivel

Una vez finalizado el ejercicio de actualización de matrices de riesgos y construido el mapa de riesgos, el Grupo de Resiliencia Operacional realizará la homologación de los riesgos con el fin de definir los riesgos de primer y segundo nivel.

El objetivo principal de definir los riesgos de primer nivel es presentar informes de seguimiento de manera agrupada generando aspectos relevantes del monitoreo y autocontrol que ejercen los procesos frente a la administración del riesgo y exponer a

la Alta Dirección, en términos generales, resultados puntuales que generen valor y que sean considerados importantes para la toma de decisiones y la asignación de recursos.

Los riesgos de primer nivel son el resultado de homologar por tipología los riesgos identificados en las 21 matrices de riesgos de los procesos del Sistema de Gestión Integrado.

Para su homologación se tiene en cuenta los siguientes pasos:

1. Se identifican las diferentes tipologías de riesgos inherentes a los procesos del Sistema de Gestión Integrado, con el fin de realizar una segregación según dicho aspecto.
2. Una vez identificados los riesgos de segundo nivel, se debe identificar las causas raíz de los riesgos segregados, con el fin de identificar características similares entre estos.
3. Se definen riesgos generales para la Entidad que contengan las características identificadas.
4. La probabilidad e impacto inherentes y residuales son el resultado calcular el promedio aritmético de los riesgos de segundo nivel según la segregación que se realiza para cada uno de los riesgos identificados.
5. El riesgo inherente y residual de cada uno de los riesgos de primer nivel resulta de la combinación de las variables probabilidad e impacto definidas previamente (promedio de riesgos de segundo nivel), según los niveles de riesgos establecidos en la metodología de riesgos de la Entidad.
6. Los perfiles de riesgo inherente y residual de cada tipología de riesgos resultan de calcular el promedio de las variables de probabilidad e impacto de los riesgos de primer nivel (paso anterior), según los niveles de riesgos establecidos en la metodología de riesgos de la Entidad.

Los criterios para identificar y evaluar los riesgos de primer nivel son:

a. Los riesgos de segundo nivel homologados deben pertenecer a una misma tipología.
b. Las variables de probabilidad e impacto para cada uno de los riesgos de primer nivel deben ser calculadas a través de promedios aritméticos y asignadas según las escalas definidas en la metodología de riesgos de la Entidad.
c. La definición de los riesgos de primer nivel se realiza de manera cualitativa, identificando las características comunes entre los riesgos de segundo nivel segregados para cada tipología.
d. Se debe considerara la estructura establecida en la metodología de riesgos para la definición de riesgos.
e. Se deben definir riesgos de primer nivel que permitan contemplar todos los riesgos claves de la Entidad.
f. El análisis cualitativo impondrá un ajuste en la descripción del riesgo, utilizando términos que cobijen elementos propios de la Entidad. Ejemplo: Servicios de TI contempla, comunicación, internet, software, hardware, etc.

La materialización de un riesgo de según nivel, inmediatamente, deriva en la materialización del riesgo de primer nivel al que pertenece.

Se realizará el seguimiento al total de los riesgos identificados, pero de acuerdo con el resultado de la homologación realizada, se presentará el seguimiento a nivel general y se destacarán los aspectos que requieran ser revisados en los comités institucionales.

8. CRITERIOS PARA LA ACTUALIZACIÓN Y OFICIALIZACIÓN DE MATRICES DE RIESGOS

Cuando los cambios realizados en la metodología de riesgos lo ameriten o dentro del año siguiente de la versión actual de la matriz de riesgos del proceso, se debe realizar la actualización de esta, la cual tiene como objetivo monitorear los riesgos identificados en anteriores ejercicios, para evaluar la modificación, eliminación o inclusión de nuevos riesgos. Para realizar la actualización de matrices, es necesario consultar previamente los criterios y lineamientos definidos en la metodología de riesgos aprobada en el aplicativo SGI.

Cuando los procesos decidan realizar actualización a su matriz de riesgos, en cualquier momento del año, es necesario que soliciten al Grupo de Resiliencia Operacional la actualización del inventario de controles, previo a la realización de los ajustes sobre la proforma interna. Para esto se deberá enviar la solicitud al correo resiliencia.operacional@superfinanciera.gov.co, con la matriz de riesgos vigente adjunta. El Grupo de Resiliencia Operacional contara con dos (2) días hábiles para realizar la actualización de la hoja “INVENTARIO DE CONTROLES” y devolver al proceso.

Anualmente, El Oficial de Resiliencia Operacional junto con su equipo, establecen el cronograma a seguir para realizar el ejercicio de actualización de las matrices de riesgos en cada uno de los procesos del SGI, en el primer semestre del año.

El Grupo de Resiliencia Operacional debe cumplir con las siguientes funciones frente a la actualización de matrices de riesgos:

- Crear el plan de acción para el desarrollo del ejercicio de actualización de las matrices de riesgos de cada proceso.
- Socializar los ajustes realizados (cuando aplique) en la metodología de riesgos, a los Facilitadores del proceso, Coordinadores de Calidad e integrantes de la Oficina Asesora de Planeación.
- Verificar el cumplimiento de los lineamientos establecidos en la metodología de riesgos, previa oficialización de la matriz de riesgos en el aplicativo SGI. Se deben enviar por escrito las observaciones identificadas en la revisión, para que sea el proceso quien realice los ajustes en la matriz.

- Compartir con el Grupo para la Transparencia y Lucha contra la Corrupción, los riesgos de proyectos de inversión identificados por los procesos, para que sean ellos quienes realicen la respectiva revisión, con el propósito de validar que se encuentren alineados con lo definido en la MGA-Web.
- Compartir con el Grupo para la Transparencia y Lucha contra la Corrupción, los riesgos de corrupción con el fin de revisar y solicitar los ajustes que consideren necesarios.
- Verificar la oficialización de las matrices de riesgos en el SGI e informar de los hallazgos evidenciados.
- Verificar la creación de planes de acción para aquellos procesos que cumplan con alguno de los requisitos mencionados en el numeral 6.7.1 del presente documento.
- Calcular el perfil de riesgos de la Entidad y sus procesos tomando como fuente de información las matrices oficializadas en el aplicativo SGI.
- Actualizar los riesgos de primer nivel.
- Actualizar el inventario de controles
- Actualizar el Mapa de riesgos de la SFC (E-MT-PLA-007) tomando como base la información de las matrices de riesgos de cada proceso oficializada en el SGI.
- Enviar a revisión, por parte del Oficial de Resiliencia Operacional, el mapa de riesgos de la Entidad, el cual es revisado previamente por el Facilitador del proceso de Planeación.
- Solicitar aprobación del Mapa de Riesgos de la SFC al Jefe de la Oficina Asesora de Planeación y/o Líder del proceso de Planeación.
- Publicar el mapa de riesgos de la Entidad en la página web, luego de ser aprobado en el aplicativo SGI. Con el fin de cumplir con los criterios de seguridad de la información, se genera la versión limitada para publicación en el sitio web de la Entidad. Dicha publicación debe ser solicitada al Grupo de Comunicaciones, vía correo electrónico por parte del Oficial de Resiliencia Operacional, relacionando el enlace especifico.
- Recopilar las lecciones aprendidas durante el proceso de actualización de matrices de riesgo anual, con el propósito de establecer el plan de mejoramiento correspondiente para su remediación.

Es importante que los procesos, realicen la codificación de sus matrices de riesgos de acuerdo con los lineamientos establecidos en el procedimiento E-PR-PLA-001 Control de Documentos, así como el diligenciamiento del HISTORIAL DE CAMBIOS en el aplicativo SGI, en el cual se debe registrar todos los cambios realizados en cada versión de la matriz de riesgos del proceso. La nomenclatura definida para oficializar las matrices de riesgos en el SGI es: Inicial de tipo de proceso (1 carácter) - la sigla “MT” que significa matriz-siglas del proceso con las que se identifica en el SGI (3 caracteres) – consecutivo numérico (tres caracteres).

Ejemplos: E-MT-PLA-001, A-MT-GTI-001

9. LINEAMIENTOS ESPECIALES PARA OTROS RIESGOS

9.1 Riesgos de Corrupción

Para los riesgos asociados a posibles actos de corrupción, se consideran los siguientes aspectos:

- El riesgo de corrupción se define como la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- Los riesgos de corrupción se establecen sobre procesos.
- El riesgo debe estar descrito de manera clara y precisa. Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos.

Para definir si un riesgo es tipificado como de corrupción se deberá contemplar si cumple con las siguientes características:

- Existe acción u omisión
- Existe uso del poder
- Desvía la gestión de lo público
- Obtiene un beneficio privado

Para la gestión de riesgos de corrupción, se siguen los mismos criterios establecidos en la metodología de riesgos de gestión, sin embargo, existen algunos aspectos especiales a tener en cuenta:

a. Para la codificación del riesgo, se debe iniciar con las iniciales del proceso seguido de la sigla "COR" y finaliza con el consecutivo que asigne el proceso. Ejemplo: PLA_COR_001, DJU_COR_002, DDS_COR_003.

b. La variable probabilidad de ocurrencia, se determina teniendo en cuenta qué tan posible es que ocurra el riesgo, expresado en términos de frecuencia (número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo) o factibilidad (presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado, pero es posible que suceda).

Los niveles de probabilidad para este tipo de riesgos se definen considerando la siguiente tabla:

Tabla 5. Cálculo de la probabilidad riesgos de corrupción

Tabla de Probabilidad de Ocurrencia			
Nivel	**Nivel**	**Descripción**	**Frecuencia**
5	**Muy Alta**	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de una (1) vez al año.

4	**Alta**	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos una (1) vez en el último año.
3	**Media**	El evento podrá ocurrir en algún momento.	Al menos una (1) vez en los últimos dos (2) años.
2	**Baja**	El evento puede ocurrir en algún momento.	Al menos una (1) vez en los últimos cinco (5) años.
1	**Muy Baja**	El evento puede ocurrir solo en circunstancias excepcionales (Poco comunes o anormales).	No se ha presentado en los últimos cinco (5) años.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas – DAFP

c. Para definir la variable impacto en estos riesgos, el proceso debe diligenciar, en la hoja "D. IMPACTO CORRUPCIÓN" de la proforma interna, el cuestionario definido para tal fin. De acuerdo con el resultado final de las respuestas positivas, el nivel de impacto estará por:

Respuestas afirmativas de 1 a 5 pregunta(s)= Impacto moderado
Respuestas afirmativas de 6 a 11 preguntas= Impacto mayor
Respuestas afirmativas de 12 a 19 preguntas= Impacto catastrófico

Es importante considerar que para este tipo de riesgos no aplican los niveles de impacto leve y menor. Por lo anterior, el nivel de riesgo inherente y residual para este tipo de riesgo no puede ser inferior a Moderado.

d. En este tipo de riesgo, no es posible implementar controles de tipo correctivo, dado que estos buscan disminuir la variable impacto y dada la naturaleza del riesgo no es posible generar desplazamiento en esta.

e. Los riesgos de corrupción no admiten como tratamiento del riesgo la opción de aceptar, dada la naturaleza e implicaciones de este. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad.

El Grupo para la Transparencia y Lucha contra la Corrupción es el encargo de establecer acciones para el tratamiento de los riesgos de corrupción en todos los niveles de la Entidad.

f. Desde el grupo de Grupo para la Transparencia y Lucha contra la Corrupción se realiza acompañamiento en la definición, análisis y valoración de los riesgos de corrupción, así como el respectivo seguimiento y actualización del mapa con la periodicidad definida.

g. Los lideres de proceso serán los responsables de identificar, medir, tratar y monitorear los riesgos de corrupción, al menos una vez al año.

h. El resultado de la identificación y la evaluación de los riesgos de corrupción es consolidado por la Oficina Asesora de Planeación y es fuente principal para la generación del mapa de riesgos de corrupción, el cual se encuentra publicado en la página web de la Entidad.

El mapa de riesgos de corrupción es publicado para comentarios de la ciudadanía en la página web de la entidad. Se debe dejar por escrito la evidencia de las modificaciones o ajustes que se realicen al mapa de riesgos de corrupción.

i. Durante el seguimiento anual, los procesos deben aplicar una autoevaluación de los riesgos de corrupción, en la proforma interna E-PI-PLA-018 Plantilla Contexto Organizacional y Matriz de Riesgos para validar que los controles sean efectivos frente a la mitigación y prevención de las causas que dan origen a los posibles eventos identificados, lo anterior, de acuerdo con lo definido en el artículo 55 de la Ley 2195 de 2022.

Los lideres de procesos son responsables de informar al Grupo de Transparencia y Lucha contra la Corrupción, la materialización de los riesgos de este tipo, con el fin de establecer en conjunto a las acciones de respuesta para mitigar el impacto de este.

9.2 Riesgos de Seguridad de la Información

Para la gestión de los riesgos de seguridad de la información se debe tener en cuenta la seguridad de la información y la ciberseguridad, la cual se vincula al Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC, a su vez alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital: seguridad de la información, arquitectura, servicios ciudadanos digitales.

Para identificar los riesgos asociados a seguridad digital, es necesario contemplar los activos de Información críticos para el proceso y cómo éstos pueden ser vulnerados en alguno de los principios de la seguridad de la Información: Confidencialidad, Integridad y Disponibilidad.

Los riesgos inherentes a la seguridad de la información se clasifican en:

- Pérdida de confidencialidad
- Pérdida de integridad
- Pérdida de disponibilidad
- No repudio (origen/destino)

Para el caso de los riesgos de Seguridad digital y Ciberseguridad, la sola presencia de una vulnerabilidad no causa daños por sí misma, dado que es necesario que exista una amenaza presente para explotarla. Una **vulnerabilidad** que no tiene una amenaza puede no requerir la implementación de un control.

Un ejemplo de un riesgo de seguridad digital, suministrado por el DAFP, es: Posibilidad de pérdida de la integridad de la información. Descripción: La falta de lineamientos de seguridad digital, ausencia de políticas de control de acceso, contraseñas sin protección y mecanismos de autenticación débil, pueden facilitar una modificación no autorizada causando la pérdida de la integridad de la base de datos de nómina.

Para la gestión de riesgos de Seguridad Digital, se siguen los mismos criterios establecidos en la metodología de riesgos de gestión, sin embargo, existen algunos aspectos especiales a tener en cuenta:

a. La probabilidad e impacto de los riesgos de seguridad de la información se determinan de acuerdo con la amenaza no con las vulnerabilidades.

b. Durante la caracterización del riesgo en la hoja "C. RIESGOS" en la proforma interna, al seleccionar el tipo de riesgo Seguridad de la Información, se habilitarán los campos Activos, Amenaza y Vulnerabilidad, los cuales se deben diligenciar de acuerdo con:

Activos impactados (Qué)

Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital son activos digitales, que utiliza la Entidad para funcionar en el entorno digital incluido el ciberespacio, tales como: Aplicaciones de la organización, Servicios Web, Redes, Información Física o digital, Tecnologías de la Información y Tecnologías de Operación.

De acuerdo con el análisis realizado, con apoyo del Grupo de Resiliencia Operacional, se contemplan la priorización de los siguientes activos (en términos generales) para garantizar la atención al ciudadano, proteger y garantizar su funcionamiento y la relación con los grupos de valor o partes interesadas:

- Funcionarios
- Información
- Instalaciones
- Hardware
- Software
- Red
- Imagen

Amenazas

Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas y, por lo tanto, a la Entidad. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas, por lo tanto, es

recomendable identificar todos los orígenes de las amenazas accidentales como deliberadas.

Las amenazas se deberán identificar genéricamente y por tipo, como por ejemplo Acciones no autorizadas, daño físico, fallas técnicas, cibercriminal.

Como apoyo para la definición de amenazas se puede tomar como referencia la hoja “AMENA y VULNE CIBER“, disponible en la proforma internaE-PI-PLA-018.

Vulnerabilidades (por qué y cómo)

Una vulnerabilidad es una debilidad que puede permitir el ingreso de un agente externo facilitando que un atacante cibernético tenga acceso no autorizado a la información reservada de la Entidad, Para identificar las vulnerabilidades es importante conocer las amenazas comunes, así como el inventario de activos de información.

Se pueden identificar vulnerabilidades en los siguientes temas:

- Organización.
- Procesos y procedimientos.
- Personal
- Ambiente físico
- Configuración del sistema de información.
- Hardware, software y equipos de comunicaciones.
- Dependencia de partes externas.

Como apoyo para la definición de amenazas se puede tomar como referencia la hoja “AMENA y VULNE CIBER“, disponible en la proforma internaE-PI-PLA-018.

La identificación de activos, amenazas y vulnerabilidades para este tipo de riesgos se realiza con el apoyo del Grupo de Resiliencia Operacional.

c. Para la definición de controles se puede tomar como guía el Anexo A - ISO 27001-2013, el cual se encuentra disponible en la hoja “CONTROLES SEGDIG” de la proforma interna E-PI-PLA-018.

9.3 Riesgos de Ciberseguridad

La identificación, medición, control, tratamiento y monitoreo de los riesgos de ciberseguridad en toda la Entidad, es realizada por el Grupo de Resiliencia Operacional, con apoyo de la Dirección de Tecnologías de la Información.

La identificación de riesgos cibernéticos se realiza a partir de los riesgos de seguridad digital y los activos identificados por los procesos en la hoja C. RIESGOS, donde se toma como referencia la hoja “AMENA y VULNE CIBER“, disponible en la proforma interna E-PI-PLA-018.

Para la gestión de riesgos de Ciberseguridad, se siguen los mismos criterios establecidos en la metodología de riesgos de gestión, sin embargo, existen algunos aspectos especiales a tener en cuenta:

a. Durante la actualización de matrices de riesgos realizada de manera anual, el Grupo de Resiliencia Operacional actualiza los riesgos, causas y controles de ciberseguridad y los incluye en la hoja C.RIESGOS de las matrices de riesgos de cada uno de los procesos según corresponda, de acuerdo a lo definido en los riesgos de seguridad digital del proceso.

b. El Grupo de Resiliencia Operacional es el responsable de diligenciar la hoja F. CIBER, de acuerdo con la identificación de los riesgos cibernéticos del proceso.

c. El seguimiento a la gestión de los riesgos de Ciberseguridad, lo debe realizar el Facilitador de cada proceso, con el apoyo del Coordinador de Calidad del proceso.

d. Para facilitar la identificación de riesgos cibernéticos, se deben identificar los siguientes elementos previo a la definición del riesgo ciber:

- Objetivo del proceso
- Activos cibernéticos amenazados
- Amenazas
- Agentes generadores (quién)
- Motivos: Económicos, religiosos o políticos.
- Capacidades: Conocimientos, financiamiento o tamaño.
- Intenciones: Diversión, crimen o espionaje.
- Vulnerabilidad: Debilidades que presenta el activo cibernético.

e. En la identificación de riesgos de ciberseguridad, se deben contemplar los riesgos a los que están expuestos los proveedores de la cadena de suministros que presten servicios a través del ciberespacio.

9.4 Riesgos de Proyectos de Inversión

Para la gestión de riesgos de Proyectos de Inversión, se siguen los mismos criterios establecidos en la metodología de riesgos de gestión, sin embargo, es importante considerar que, para la identificación de estos riesgos, se deberá tener en cuenta la articulación con los riesgos incluidos en la Metodología General Ajustada – MGA Web.

Adicionalmente, los procesos que cuenten con proyectos vigentes deberán considerar al menos un riesgo de este tipo.

La revisión y pertinencia de estos riesgos está a cargo del Grupo para la Transparencia y Lucha contra la Corrupción.

9.5 Riesgos de Continuidad

El Sistema de Gestión de Continuidad del Negocio busca fortalecer a la Entidad para prepararse ante las emergencias, a gestionar las crisis y mejorar su capacidad de recuperación operacional, con el fin de asegurar la cadena de suministro y evitar las pérdidas ante una crisis.

La identificación y el análisis de este tipo de riesgo ser realiza contemplando el Análisis de Impacto al Negocio (BIA, por sus siglas en inglés) del proceso.

La definición del riesgo, las causas y los controles, serán propuesto por el Grupo de Resiliencia Operacional a los procesos, para que sean ellos quienes definan la pertinencia de estos dentro de la gestión de los riesgos del proceso.

No obstante, es obligatorio contemplan riesgos de continuidad en aquellos procesos que son considerados y categorizados como de línea critica.

9.6 Riesgos de Lavado de Activos, Financiación del Terrorismo y la Financiación de la Proliferación de Armas de Destrucción Masiva

El lavado de activos (LA), la financiación del terrorismo (FT) y la financiación de la proliferación de arma de destrucción masiva (FPADM) representan una amenaza para la estabilidad y reputación de la Entidad, lo que fomenta el establecimiento de estrategias, políticas y directrices para la adecuada gestión de este riesgo.

La gestión frente al riesgo LAFT/FPADM, brinda elementos a todos los vinculados, que permitan prevenir que la Entidad sea utilizada como instrumento para la realización de operaciones de lavado de activos y/o canalización de recursos hacia la realización de actividades ilícitas.

El alcance inicial en las actividades para los riesgos de Lavado de Activos y Financiación del Terrorismo se enmarca en la identificación de terceros para las actividades de contratación, nombramiento y reuniones.

El detalle de los lineamientos sobre riesgos de Lavado de Activos y Financiación del Terrorismo se encuentra en el Manual Operativo de Lineamientos Transversales en Resiliencia (E-MN-PLA-008).

Los procesos deberán identificar la existencia de riesgos de este tipo en las actividades que desarrollan, y aplicar los lineamientos definidos en la presente metodología para su gestión.

9.7 Riesgos Emergentes y/o No Identificados

Los riesgos emergentes son aquellos considerados como los riesgos que actualmente no existen o que aún no se reconocen, pero que podrían surgir a raíz de cambios en

el entorno. Para dichos riesgos, no aplica los mismos criterios mencionados anteriormente, porque su frecuencia y sus consecuencias son desconocidas. No obstante, la experiencia muestra que cuando se materializan, tienen un impacto significativo y, por lo tanto, no se pueden ignorar.

Por lo anterior, los procesos frente a la gestión que hacen de los riesgos asociados, deberán identificar cuáles son las amenazas que posiblemente se pueden materializar y que aún no se encuentran incluidas en las matrices de riesgos, dado que si este nace de una actividad que no se ha contemplado en la caracterización del proceso, esta información deberá ser actualizada en las diferentes herramientas de gestión con el fin de controlar aquello que aunque se realiza día a día y se controla, no se tiene documentado formalmente, por lo que la Entidad no podrá tomar acciones pertinentes que puedan ayudar a subsanar las situaciones en caso de que algo pueda ocurrir y por lo tanto afectar a la operatividad de la Entidad.

En caso de que el proceso identifique estos riesgos no documentados, deberán realizar el análisis del tipo de riesgo al que corresponde, para de esta manera proceder con la respectiva aplicación de criterios de acuerdo con lo señalado en el presente documento. La información deberá ser canalizada a través de los Coordinadores de Calidad de los Procesos y posteriormente se realizará la revisión y validación de la información desde el Grupo de Resiliencia Operacional.

ANEXOS

ANEXO 1. Términos y Definiciones

- **Amenazas:** Causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización. Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas y, por lo tanto, a la Entidad.
- **Análisis de riesgos:** Proceso sistemático para entender la naturaleza del riesgo y evaluar la criticidad de reducir el nivel del riesgo.
- **Apetito de riesgo:** Es el nivel de riesgo que la Entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la Entidad debe o desea gestionar.
- **Calidad:** Grado en el que un conjunto de características inherentes cumple con los requisitos.
- **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 y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.
- **Causas o factores de riesgos:** Son los medios, circunstancias y agentes que generan los riesgos. Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **Causa Inmediata**: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

- **Causa Raíz:** Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.
- **Ciberseguridad**: Preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio.
- **Coordinador del Proceso** funcionario designado por el Jefe de la Oficina Asesora de Planeación y/o Líder del proceso de Planeación para realizar labores de apoyo y acompañamiento metodológico en la elaboración y seguimiento de las matrices de riesgos de los procesos que componen el Sistema de Gestión Integrado.
- **Compartir el riesgo**: Compartir con otra de las partes el peso de la pérdida o del beneficio de la ganancia proveniente de un riesgo particular a fin de reducir la probabilidad o el impacto de su materialización.
- **Confidencialidad**: Hace referencia a la protección de información cuya divulgación no está autorizada.
- **Consecuencia**: Resultado o impacto de un evento que afecta los objetivos Una consecuencia puede ser cierta o incierta y puede tener efectos positivos o negativos en los objetivos.
- **Control:** Medida que permite reducir o mitigar un riesgo, su implementación y monitoreo está a cargo de los dueños de los procesos.
- **Disponibilidad**: se define como la capacidad de mantener la información clara y accesible en el momento que se requiera, al igual que los recursos necesarios para su uso.
- **Evaluación del control:** Revisión sistemática de los procesos para garantizar que los controles aún son eficaces y adecuados.
- **Evaluación del riesgo:** Proceso de comparar el nivel de riesgo frente a los criterios del riesgo.
- **Evento**: Ocurrencia de un conjunto particular de circunstancias. En ocasiones, se puede hacer referencia a un evento como un “incidente “o “accidente”. También se puede hacer referencia a un evento sin consecuencias, como un cuasi- accidente, incidente, situación de peligro o conato de accidente.
- **Evitar el riesgo**: Decisión de no involucrarse en o retirarse de una situación de riesgo.
- **Frecuencia**: Medición del número de ocurrencias por unidad de tiempo.
- **Gestión del Riesgo**: un proceso efectuado por la alta dirección de la Entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.
- **Identificación del riesgo**: Proceso para determinar qué, cuándo, dónde, porqué y cómo podría suceder un evento que podría afectar el cumplimiento de las actividades y objetivos de cada proceso, con base en esto, se analiza, se identifica y se valora el riesgo.
- **Indicador**: Expresión cualitativa o cuantitativa observable, que permite describir características, comportamientos o fenómenos de la realidad a través de la evolución de una variable o el establecimiento de una relación entre variables, la que, comparada con períodos anteriores, productos similares o una meta o compromiso, permite evaluar el desempeño y su evolución en el tiempo.
- **Integridad:** La información debe ser precisa, exacta desde su creación hasta su destrucción.

- **Impacto**: se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Nivel de riesgo:** Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.
- **Mapa de riesgos:** Herramienta metodológica que permite hacer un inventario de los riesgos detallando la descripción de cada uno de éstos y las posibles consecuencias.
- **Monitorear**: Verificar, supervisar, observar críticamente o medir regularmente el progreso de una actividad, una acción o un sistema para identificar los cambios en el nivel de desempeño requerido o esperado.
- **Plan de contingencia**: Parte del plan de manejo de riesgos que contiene las acciones a ejecutar en caso de la materialización del riesgo, con el fin de dar continuidad a la operación y logro de los objetivos de la Entidad.
- **Plan de manejo o tratamiento del riesgo**: Plan de acción propuesto por el grupo de trabajo.
- **Probabilidad:** Se entiende la posibilidad de ocurrencia del riesgo, ésta puede ser medida con criterios de Frecuencia o Factibilidad.
- **Reducción del riesgo:** Acciones que se toman para disminuir la posibilidad, las consecuencias negativas, o ambas, asociadas con un riesgo.
- **Responsables:** Son las dependencias o áreas encargadas de adelantar las acciones propuestas.
- **Riesgo:** Efecto que se causa sobre los objetivos de la Entidad, debido a eventos potenciales que puedan 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.
- **Riesgo de Gestión**: Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.
- **Riesgo Inherente:** Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.
- **Seguimiento**: Recolección regular y sistemática sobre la ejecución del plan, qué sirven para actualizar y mejorar la planeación futura.
- **Sistema de Gestión de Calidad**: Sistema de gestión para dirigir y controlar una organización con respecto a la calidad.
- **Sistema de Gestión de Ciberseguridad:** Sistema de gestión basada en un conjunto de normas que permite identificar, atender y minimizar los riesgos que puedan atentar contra la integridad, confidencialidad y disponibilidad de la información en el ciberespacio de una organización.
- **Sistema de Gestión de Continuidad del Negocio**: Sistema de gestión que busca ayudar a las organizaciones a prepararse para las emergencias, a gestionar las crisis y mejorar su capacidad de recuperación operacional, asegurar la cadena de suministro y protegerse, por ejemplo, su reputación ante una crisis.
- **Sistema para la gestión de riesgo:** Conjunto de elementos del sistema de gestión de una organización involucrados en la gestión de riesgo.
- **Sistema de Seguridad de la Información**: Sistema de gestión que, por medio de definición, implementación y mantenimiento de políticas y procedimientos, busca

preservar la confidencialidad, integridad y disponibilidad de la información de una organización.

- **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.
- **Valoración del riesgo**: Proceso total de identificación del riesgo, análisis del riesgo y evaluación del riesgo.

  Vulnerabilidades: Debilidad o debilidades presentes en los sistemas de información, procesos, equipos, procedimiento o en la calidad de controles, que pueden ser aprovechadas con el fin de causar daño a un activo de información.

Historial de cambios

FECHA	VERSIÓN	CAMBIOS
18/03/2022	1	Versión inicia
15/09/2022	2	Se eliminó la referencia “#LaSuperSomosTodos”
31/10/2022	3	Se incluye al líder del proceso de planeación en los numerales 1.6, 1.6.3.2 y en el anexo 1 términos y definiciones.
4/112022	4	Se realiza ajuste general a la redacción de la metodología. Se reorganiza la estructura de los ítems del documento con el fin de facilitar su entendimiento. Se ajusta el documento considerando los cambios realizados en la nueva proforma interna E-PI-PLA-018-Plantilla Contexto Organizacional y Matriz de Riesgos. Se involucra la gestión integral de riesgos como parte del modelo ERM. Se incluye en el contexto organizacional de la SFC. Se incluye los grupos de valor de la SFC Se ajusta la definición de estrategias DOFA. Se ajusta y unifica la codificación de riesgos, causas y controles Se incluyen lineamientos relacionados con la administración del inventario de controles. Se incorporan los criterios para la priorización de riesgos. Se especifican los criterios a considerar para cada uno de los seguimientos de riesgos. Se documentan los canales de comunicación para el reporte de situaciones de riesgo. Se ajusta y define el flujo para el item “Reporte de Eventos de Riesgos y/o Materialización de riesgos”. Se definen los criterios a considerar para el establecimiento de Planes de mejora para la gestión del riesgo en el SGI Se indica los criterios para la definición de los Riesgos de Primer nivel Se ajustan las responsabilidades del Grupo de Resiliencia Operacional frente a la actualización y oficialización de matrices de riesgos Se incluye el control documental y el manejo del inventario de controles para la oficialización de matrices de riesgo, De acuerdo con los criterios del documento E-PR-PLA-001 Control de Documentos. Se especifican y ajustas los cambios en la metodología de riesgos de gestión para otros riesgos específicos.