ADMINISTRADORA DE LOS RECURSOS DEL SISTEMA
GENERAL DE SEGURIDAD SOCIAL EN SALUD

MANUAL PARA LA GESTIÓN DE RIESGOS

ADMINISTRADORA DE LOS RECURSOS DEL SISTEMA GENERAL DE SEGURIDAD SOCIAL EN SALUD

BOGOTÁ, FEBRERO DE 2024

TABLA DE CONTENIDO

LISTA DE TABLAS

TABLA DE FIGURAS

1. OBJETIVO

Establecer la metodología de administración de riesgos de gestión, corrupción y de Lavado de Activos y Financiación del Terrorismo - LA/FT, seguridad de la información, crédito, liquidez y mercado, de acuerdo con los lineamientos de la guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 6 del Departamento Administrativo de la Función Pública y la Circular 06 de 2018 emitida por la Superintendencia Nacional de Salud; mediante la identificación, análisis y valoración, establecimiento de controles, tratamiento y monitoreo a los riesgos que puedan afectar negativamente la gestión de los procesos de la Administradora de los Recursos del Sistema de Seguridad Social en Salud - ADRES en su modelo integrado de planeación y gestión institucional.

2. ALCANCE

Aplica a todos los procesos de la ADRES, en su modelo integrado de planeación y gestión institucional y en todos los niveles de la organización, con el esquema de líneas de defensa para administrar los riesgos de gestión, corrupción y de Lavado de Activos y Financiación del Terrorismo-LA/FT, seguridad de la información, crédito, liquidez y mercado. Iniciando con la identificación de riesgos siguiendo con el análisis, valoración, definición de controles, tratamiento y finaliza con el monitoreo, seguimiento y comunicación.

El presente manual es de obligatorio cumplimiento para los todos los colaboradores de la entidad.

3. DOCUMENTOS ASOCIADOS AL MANUAL

Caracterización del Proceso de Direccionamiento Estratégico DIES-CP01.
Política de Administración de Riesgos DIES-PL01
Política de Debida Diligencia DIES-PL02
Procedimiento Administración de Riesgos DIES-PR02
Procedimiento Reporte de Operaciones Inusuales o Sospechosas – SARLAFT DIES-PR06
Procedimiento Gestión de Activos de Información OSTI-PR08.
Procedimiento Gestión de la Seguridad de la Información OSTI-PR09.
Metodología de clasificación y valoración de activos de información OSTI-GU01.
Matriz de Valoración de Activos de Información OSTI-FR02.
Formato Mapa de Riesgos Consolidado de la ADRES DIES-FR16
Matriz de Vulnerabilidad de Procesos DIES-FR18

4. NORMATIVA Y OTROS DOCUMENTOS EXTERNOS

Ley 1712 de 2014, Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

Ley 1474 de 2011 "Por el cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública", señalando en su artículo 73 reglamentado por el Decreto 264 de 2012, que "cada entidad

del orden nacional, departamental y municipal deberá elaborar anualmente una estrategia de lucha contra la corrupción y de atención al ciudadano. Dicha estrategia contemplará, entre otras cosas, el mapa de riesgos de corrupción en la respectiva entidad, las medidas concretas para mitigar esos riesgos, las estrategias anti-trámites y los mecanismos para mejorar la atención al ciudadano. El Programa Presidencial de Modernización, Eficiencia, Transparencia y Lucha Contra la Corrupción señalará una metodología para diseñar y hacerle seguimiento a la señalada estrategia".

Ley 527 de 1999, por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

Ley 489 de 1998 "Por la cual se dictan normas sobre la organización y funcionamiento de las entidades del orden nacional, se expiden las disposiciones, principios y reglas generales para el ejercicio de las atribuciones previstas en los numerales 15 y 16 del artículo 189 de la Constitución Política y se dictan otras disposiciones".

Ley 87 de 1993 "Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones".

Constitución Política "Principios de la Función Administrativa y Mecanismos de Control" – artículos 209 y 269.

Decreto 1499 de 2017 "Por medio del cual se modifica el Decreto número 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".

Decreto 1083 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública", señalando en su artículo 2.2.21.5.3, modificado por el artículo 17 del Decreto 648 de 2017, que "las Unidades u Oficinas de Control Interno o quien haga de sus veces desarrollarán su labor a través de los siguientes roles: liderazgo estratégico; enfoque hacia la prevención, evaluación de la gestión del riesgo, evaluación y seguimiento, relación con entes externos de control". Su artículo 2.2.21.5.4 también determina que la administración de riesgos es parte integral del fortalecimiento de los sistemas de control interno en las entidades públicas y que en ese sentido, las autoridades deben establecer y aplicar políticas de administración del riesgo a través de un "proceso permanente e interactivo entre la administración y oficinas de control interno o quien haga de sus veces, evaluando los aspectos tanto interno como externos que pueden llegar a representar amenaza para la consecución de los objetivos organizacionales, con miras a establecer acciones efectivas, representadas en actividades de control, acordadas entre los responsables de las áreas o procesos y las oficinas de control interno e integradas de manera inherente a los procedimientos." El artículo 2.2.22.2.1, sustituido por el artículo 1º del Decreto 1499 de 2017, contempla, entre otras, a la "Transparencia, acceso a la información pública y lucha contra la corrupción" como una de las políticas de Gestión y Desempeño institucional y que su implementación se hará a través de planes, programas, proyectos, metodologías y estrategias.

Decreto 943 de 2014 "Por él se actualiza el Modelo Estándar de Control Interno (MECI).

Decreto 2482 de 2012 "Por el cual se establecen los lineamientos generales para la integración de la planeación y la gestión"

Circular 000006 de 2018, de la Superintendencia Nacional de Salud, por la cual se hacen modificaciones a la circular 047 de 2007 en lo relacionado con el sistema integrado de gestión de riesgos y a sus subsistemas de administración de riesgos y reporte de información.

Estándares de referencia

Norma ISO 31000 2018, Norma internacional que proporciona principios y directivas eficaces para el tratamiento y la gestión de riesgos.
Norma Técnica ISO 27001:2013 Tecnología de la información. técnicas de seguridad. sistemas de gestión de la seguridad de la información. Requisitos.

Otros documentos

Modelo de Seguridad y Privacidad de la Información, Versión 4 – Ministerio de Tecnologías de la Información y las Comunicaciones febrero 2021.
Guía para la administración del riesgo y el diseño de controles en entidades públicas, Versión 6 – Función Pública noviembre de 2022.

5. DEFINICIONES

Conceptos básicos relacionados con el riesgo de acuerdo con "la guía para la administración de riesgos y el diseño de controles en entidades públicas versión 6 de la función pública":

Activo: en el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

Amenazas: situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

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 debo o desea gestionar.

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.

Causa: 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.

Confidencialidad: propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

Consecuencia: efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Control: medida que permite reducir o mitigar un riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

Disponibilidad: propiedad de ser accesible y utilizable a demanda por una entidad.

Factores de Riesgo: son las fuentes generadoras de riesgo.

Gestión del riesgo: 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.

Impacto: consecuencias que puede ocasionar a la organización la materialización del riesgo.

Integridad: propiedad de exactitud y completitud.

Mapa de riesgos: documento con la información resultante de la gestión de los riesgos.

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. En general la fórmula del Nivel del Riesgo poder ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.

Opacidad: La opacidad es la carencia de prácticas claras, precisas, fácilmente discernibles y aceptadas. El entendimiento de este concepto se facilita en la medida en que se reconoce su opuesto, el ideal en el marco de la buena gobernanza, esto es, la transparencia. Transparencia significa abrir la información de las organizaciones políticas y burocráticas al escrutinio público, mediante sistemas de clasificación y difusión que reducen los costos de acceso a la información gubernamental por parte de los ciudadanos. La transparencia no implica un acto de rendir cuentas a un destinatario específico sino la práctica de colocar la información en la vitrina pública para que los interesados puedan revisarla, analizarla, y en su caso usarla como mecanismo para sancionar en caso de que haya anomalías en su interior (Ugalde, 2002)[1].

Plan anticorrupción y de atención al ciudadano: plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.

Probabilidad: posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad. Está asociada a la exposición al riesgo del proceso o actividad que se esté analizando.

[1] Actúe Colombia, 2018. "Caracterización de riesgos y prácticas de corrupción y opacidad, e identificación de niveles de tolerancia a la corrupción en el sistema de salud colombiano", Grupo de Economía de la Salud - Universidad de Antioquia, mayo 2018. Disponible en IFRiesgosdecorrupcionyopacidad.pdf (actuecolombia.net)

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

Riesgo de crédito: se presenta cuando hay inadecuada asignación de cupos en las entidades financieras

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

Riesgo fiscal: Es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial, (ver conceptos de recursos públicos, bien público e Intereses patrimoniales de naturaleza pública).

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 de lavado de activos y financiación del terrorismo – LA/FT: posibilidad de pérdida o daño que podría sufrir la entidad al ser utilizada directamente o a través de sus operaciones como instrumento para el lavado de activos y/o canalización de recursos hacia la realización de actividades terroristas.

Riesgo de liquidez: se presenta al no contar con el suficiente flujo de caja necesario para cumplir con las obligaciones y compromisos de la ADRES oportunamente

Riesgo de mercado: surge de los cambios de las volatilidades, medidos por los cambios en el valor de las posiciones abiertas del mercado de capitales.

Riesgo de Seguridad de la Información: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Riesgo de seguridad digital: combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

Riesgo inherente: nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad

Riesgo residual: el resultado de aplicar la efectividad de los controles al riesgo inherente.

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. Para el riesgo de corrupción no hay nivel de tolerancia, es inaceptable.

Vulnerabilidad: representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

Los conceptos relacionados con la Circular 06 de 2018 de la Superintendencia Nacional de Salud se pueden consultar en el Glosario General de la ADRES.

Las definiciones de la Política General de Seguridad y Privacidad de la Información se pueden consultar en el documento APTI-PL01.

Los conceptos asociados a debida diligencia se pueden consultar en el documento DIES-PL02 Política de Debida Diligencia.

Consideraciones generales

- Las oportunidades se podrán abordar solamente en el contexto estratégico.
- Se deberán identificar y gestionar los riesgos estratégicos.
- La entidad dispondrá de los recursos necesarios para adoptar la política.
- En caso de materialización del riesgo se debe realizar el reporte de evento una vez se tenga conocimiento de este y se deberán tomar las acciones correctivas necesarias a nivel de proceso y a nivel de Entidad cuando aplique.
- Se realizan actualizaciones necesarias como resultado del monitoreo y revisión establecidos.
- Dentro de la etapa de seguimiento y evaluación se contempla el desarrollo de auditorías internas las cuales serán desarrolladas por la oficina de Control Interno.
- El proceso de identificación del riesgo es iterativo y debe estar en permanente revisión y actualización.
- Los líderes de procesos deben realizar reuniones cuatrimestralmente con los miembros de su equipo de trabajo, cuyo propósito sea:
    - Identificar y evaluar los riesgos
    - Identificar factores de riesgo para el proceso.
    - Identificar planes de mejora frente a materialización de riesgos
- Los riesgos de corrupción y de LA/FT se identifican para aquellos procesos que en su quehacer resulten con mayor vulnerabilidad a escenarios de corrupción, teniendo en cuenta que mediante la acción u omisión: a) manipulen información privilegiada, b) concedan autorizaciones, permisos o facultades o c) administren recursos. Los procesos con mayor vulnerabilidad se identifican en la matriz DIES-FR18 Matriz de vulnerabilidad de procesos.
- Los riesgos de seguridad de la información se aplican a todos los procesos de la ADRES en su Modelo de Planeación y Gestión Institucional, teniendo en cuenta la afectación de la confidencialidad, integridad y disponibilidad de los activos de información identificados.
- La herramienta definida para gestionar los riesgos en la entidad es Eureka.
- La herramienta definida por la entidad realiza los cálculos automáticos en lo relacionado a la solidez del control y la calificación del riesgo residual, conforme a los lineamientos emitidos por el Departamento Administrativo de la Función Pública.
- Para gestionar el Sistema de Administración del Riesgo de Lavado de Activos y de la Financiación del Terrorismo - SARLAFT se dispone de la Política de Debida Diligencia DIES-PL02 y del procedimiento de reporte de operaciones inusuales o sospechosas DIES-PR06
- No pueden existir riesgos transversales, sólo causas transversales

6. POLÍTICA DE GESTIÓN DE RIESGOS

La Política de Gestión de Riesgos de la Administradora de los Recursos del Sistema de Seguridad Social en Salud – ADRES puede ser consultada en el documento "DIES-PL01 Política de Gestión de Riesgos". Sin embargo, en el presente documento se presentan algunos apartados de esta política para dar mayor claridad a los conceptos y dar una explicación completa de la metodología.

La Política de Gestión de Riesgos aplica para todos los niveles, áreas y proceso de la entidad e involucra el contexto, la identificación, valoración, tratamiento, monitoreo, revisión, comunicación, consulta y el análisis de los siguientes subsistemas de administración de riesgos:

Figura 1. Subsistemas de Administración de Riesgos ADRES.

Fuente: Elaboración Propia Oficina Asesora de Planeación

a) **Operacional:** contempla los riesgos de:
   a. Gestión de procesos que puedan afectar el cumplimiento de la misión y objetivos de los procesos y su materialización puede llegar a afectar la continuidad de la operación.
   b. Estratégicos que puedan afectar el cumplimiento de objetivos y metas estratégicas
b) **Lavado de Activos, Financiación del Terrorismo y Corrupción:** contempla los riesgos:
   a. De posibles actos de corrupción descritos como la probabilidad de ocurrencia de eventos en los que se use el poder para desviar la gestión de lo público hacia un beneficio privado a causa de conflictos de interés, soborno, tráfico de influencias, etc.
   b. De Lavado de Activos y Financiación del Terrorismo (LA/FT), descritos como la posibilidad de pérdida o daño que podría sufrir la entidad al ser utilizada directamente o a través de sus operaciones como instrumento para el lavado de activos y/o canalización de recursos hacia la realización de actividades terroristas.
c) **Seguridad de la Información y Protección de Datos Personales:** contempla los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información de los

procesos de la entidad, y su materialización puede llegar a afectar la continuidad de la operación.

d) **Crédito:** se presenta cuando hay inadecuada asignación de cupos en las entidades financieras
e) **Liquidez:** se presenta al no contar con el suficiente flujo de caja necesario para cumplir con las obligaciones y compromisos de la ADRES oportunamente
f) **Mercado:** surge de los cambios de las volatilidades, medidos por los cambios en el valor de las posiciones abiertas del mercado de capitales.
g) **Fiscales:** Son aquellos que pueden causar un menoscabo, disminución, perjuicio, detrimento, pérdida, o deterioro de los bienes o recursos públicos y que estos riesgos pueden ser causados por una variedad de factores, como la corrupción, la falta de competencia de los funcionarios o contratistas, entre otros, la gestión del riesgo fiscal está vinculado al análisis general de los riesgos de la entidad, en consecuencia cada proceso debe analizar si existen e identificarlos, de acuerdo con sus actividades, contexto, y particularidades.
h) Y los demás que sean obligatorios por norma o los que la entidad decida implementar.

6.1 ALCANCE

En el marco del Modelo Integrado de Planeación y Gestión – MIPG, la presente Política de Administración de Riesgos Institucionales es aplicable a todos los niveles, dependencias y procesos de la entidad conforme con cada subsistema así:

- ✓ **Operacional:**
  - **Gestión:** todos los procesos de la entidad
  - **Estratégicos:** asociados a procesos estratégicos y riesgos relacionados con la planeación y cumplimiento de los objetivos institucionales.
- ✓ **Lavado de Activos, Financiación del Terrorismo y Corrupción:** procesos en los que se determinen con mayor vulnerabilidad.
- ✓ **Seguridad de la Información:** todos los procesos de la entidad.
- ✓ **Crédito:** procesos misionales en los que aplique
- ✓ **Liquidez:** procesos misionales en los que aplique.
- ✓ **Mercado:** procesos misionales en los que aplique.
- ✓ **Fiscales:** procesos en los que aplique.

6.2 NIVEL DE ACEPTACIÓN DEL RIESGO

Riesgos inherentes

La ADRES determina que para los riesgos que se encuentren en zona de riesgo baja, está dispuesta a aceptar el riesgo y no se requiere la documentación y valoración de los controles, sin embargo, se deben monitorear conforme a la periodicidad establecida.

Para los riesgos calificados de zona moderada a extrema, se requiere establecer los controles que lo mitiguen o lo reduzcan.

Riesgos residuales

La ADRES está dispuesta a aceptar que los riesgos residuales operacionales y de Seguridad de la Información se encuentren máximo en la zona moderada como nivel de aceptación y en la medida en que la gestión de riesgo vaya avanzando en su madurez, se traslade a la zona baja. Para los riesgos operacionales y de seguridad de la información que se ubiquen en zona moderada o baja, el líder de proceso podrá generar acciones de fortalecimiento, si así lo considera. Para los riesgos ubicados en zona altas y extremas, siempre deberán formular acciones de fortalecimiento.

Para los riesgos residuales de crédito, liquidez y mercado la zona de aceptación se da en zona de riesgo baja, por lo tanto, si se encuentra en una zona más alta se deben formular acciones de fortalecimiento a la gestión del riesgo.

Para el riesgo de LA/FT y corrupción no hay aceptación del riesgo, siempre deben conducir a formular acciones de fortalecimiento, cada vez que se revisen y actualicen los riesgos.

Periodicidad para el monitoreo de riesgos y controles

Los riesgos se deben monitorear cuatrimestralmente a través de la herramienta Eureka, de acuerdo con las fechas establecidas en la Guía de Administración del Riesgo del Departamento Administrativo de la Función Pública -DAFP.

Los riesgos materializados se deben monitorear mínimo una vez cada dos meses hasta que se dé por finalizado el plan de mejoramiento establecido y se realice una nueva valoración del riesgo. Para ello, debe realizarse la respectiva programación de monitoreo a través de la herramienta Eureka.

7. METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO

7.1 ESTABLECIMIENTO DEL CONTEXTO

En el establecimiento del contexto se definen los parámetros internos y externos que se han de tomar en consideración para la administración del riesgo (NTC ISO 31000, numeral 2,9). Se debe establecer el contexto tanto interno como externo de la entidad, además del contexto del proceso y sus activos de seguridad de la información.2

- **Contexto Estratégico**

Son las condiciones internas y del entorno, que pueden generar eventos originando oportunidades o afectando negativamente el cumplimiento de la misión y los objetivos de la Entidad.

Para esto se aplica una herramienta de análisis generalmente aceptada, denominada matriz DOFA, realizando un análisis del entorno y el ambiente organizacional, identificando dos categorías: a) factores externos (amenazas y oportunidades), siendo las primeras, las situaciones que pueden atentar contra un desempeño eficiente y las oportunidades, aquellas condiciones que pueden contribuir al logro de los resultados institucionales, b) factores internos (debilidades y fortalezas),

[2] Guía de administración de riesgos y el diseño de controles en entidades públicas V6. Función Pública

siendo las primeras, las falencias institucionales que le obstaculizan o imposibilitan el desempeño eficiente, eficaz y efectivo, y las segundas las potencialidades con que cuenta la organización para su desarrollo.

Las situaciones pueden ser:

Tabla 1. Factores que inciden en la matriz DOFA.

FACTORES INTERNOS		FACTORES EXTERNOS	
FORTALEZAS	**DEBILIDADES**	**OPORTUNIDADES**	**AMENAZAS**
Financieros		Sociales	
Personal		Políticos	
Procesos		Personas	
Tecnología		Económicos	
Estratégicos		Tecnológicos	
Comunicación Interna		Medio ambientales	
Infraestructura		Legales y Reglamentarios	

El Contexto Estratégico puede definirse a través de reuniones estratégicas y/o de planificación estratégica y se debe revisar por lo menos una vez al año, con el propósito de identificar posibles factores que permitan conocer la exposición a nuevos riesgos.

Las oportunidades enfocadas a la gestión del riesgo en contexto positivo se podrán abordar en el nivel estratégico, sin embargo, los procesos podrán establecer acciones para su gestión de manera voluntaria.

- **Contexto de proceso**

Se determinan las características o aspectos esenciales del ambiente en el cual la organización busca alcanzar sus objetivos a nivel de proceso, contempla los factores citados en la Tabla 1. Como parte del análisis de contexto se revisan los siguientes elementos relacionados a la gestión del proceso:

- ✓ **Diseño del proceso:** claridad en la descripción del alcance y objetivo del proceso.
- ✓ **Interacciones con otros procesos:** relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.
- ✓ **Transversalidad:** procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.
- ✓ **Procedimientos asociados:** pertinencia en los procedimientos que desarrollan los procesos.
- ✓ **Responsables del proceso:** grado de autoridad y responsabilidad de los funcionarios frente al proceso.
- ✓ **Comunicación entre los procesos:** efectividad en los flujos de información determinados en la interacción de los procesos.
- ✓ **Activos de seguridad de la información:** información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso, como de cara al ciudadano.

Se aplica la matriz DOFA o FODA, realizando un análisis del entorno y el ambiente organizacional, identificando dos categorías: a) factores externos (amenazas y oportunidades) y b) factores internos (debilidades y fortalezas).

Posterior a la consolidación de los resultados obtenidos en las debilidades y amenazas se realiza un análisis de los factores que pueden tener un mayor impacto en el cumplimiento del objetivo del proceso.

7.2 IDENTIFICACIÓN DE RIESGOS

Esta etapa tiene como objetivo identificar los riesgos que estén o no bajo el control de la organización, teniendo en cuenta el contexto estratégico en el que opera la entidad, la caracterización de cada proceso que contempla su objetivo y alcance, y el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.

Durante esta etapa, en paralelo a la identificación del evento de riesgo, se identifican las causas que dan origen al mismo.

- **Riesgos Operativos, de Crédito, Liquidez y Mercado**

Para identificar de manera adecuada los riesgos, centrándose en los aspectos determinantes para el cumplimiento de los objetivos de los procesos de la entidad o los riesgos asociados al tema de corrupción, se debe tener en cuenta el contexto estratégico y la consulta y análisis de la siguiente información:

Tabla 2. Pasos para la identificación de riesgos operativos, de crédito, liquidez y mercado.

Paso		Descripción	Fuente de información
1	Revisar el objetivo del plan o de proceso	Qué hace el proceso, para qué lo hace y cómo lo hace.	Plan Estratégico Institucional Caracterización del proceso
2	Revisar los productos finales del proceso o del plan	Revisar cuáles son los productos y/o servicios finales que se generan durante la ejecución del plan o proceso.	Plan Estratégico Institucional Caracterización del proceso
3	Determinar las características o requisitos que deben cumplir los productos identificados	Identificar cuáles son los atributos o características específicas que debe tener cada uno de los productos y/o servicios generados por el plan o proceso	Plan Estratégico Institucional Documentos del proceso
4	Revisar otros aspectos importantes	Revisar experiencias pasadas, PQRSD de los grupos de valor, riesgos materializados recientemente, problemas generados en la entidad o en el proceso, informes y conceptos de expertos, informes de la Oficina de Control Interno y entes de control, entre otros.	Informes de gestión Informes de auditoría Informes PQRSD

Fuente: Elaboración Propia Oficina Asesora de Planeación

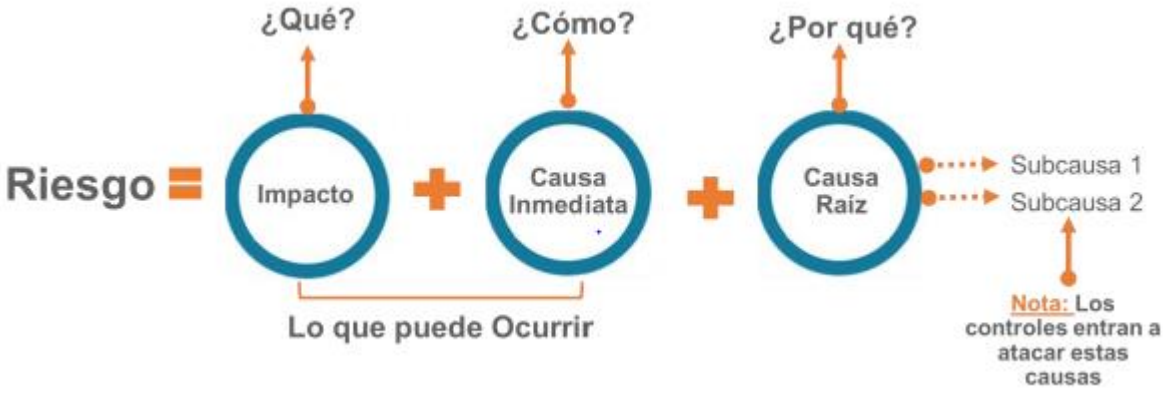
Del análisis anterior se identifican las causas y los puntos de riesgo que son aquellas actividades dentro del flujo del proceso donde existe evidencia o se tiene indicios de que pueden ocurrir eventos

de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.

Una vez identificado el posible evento, se determina el área de impacto, que es la consecuencia a la cual se ve expuesta la organización en caso de materializarse un riesgo. Para el caso de los riesgos de gestión, el área de impacto se mide como la posibilidad de afectación **económica** (presupuestal) o **reputacional.**

Con los anteriores elementos ya identificados se procede a redactar el riesgo teniendo en cuenta las preguntas **¿Qué? ¿Cómo? ¿Por qué?:**

Figura 2 - Redacción de riesgos.



Fuente: Guía para la administración del riesgo y diseño de controles – DAFP. Versión 6

Tabla 3. Estructura y ejemplo para definir el riesgo operativo, crédito, mercado y liquidez.

Área de impacto - ¿Qué?	Posibilidad afectación económica
Causa inmediata - ¿Cómo?	por multa o sanción del ente regulador
Causas raíz – ¿Por qué?	debido a adquisición de bienes y servicios fuera de los requerimientos normativos
Riesgo	Posibilidad afectación económica por multa o sanción del ente regulador debido a adquisición de bienes y servicios fuera de los requerimientos normativos

Fuente: Guía para la administración del riesgo y diseño de controles – DAFP. Versión 6

Nota: Al definir el riesgo, es importante determinar si el riesgo identificado afecta directamente el cumplimiento del objetivo del proceso u objetivos estratégicos de la Entidad. Si la respuesta es "no", este puede ser la causa o la consecuencia.

- **Riesgos de Corrupción y LAFT:**

Es 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

Es necesario que en la descripción del riesgo concurran los componentes de su definición, así:

Acción u omisión + uso del poder + desviación de la gestión de lo público + el beneficio privado

A través de la gestión eficiente de los riesgos de corrupción, se previene que la entidad pueda ser usada para dar apariencia de legalidad a dineros o recursos provenientes del posible delito de lavado de activos y financiación del terrorismo (LA/FT). A continuación, se define una estructura y se muestra un ejemplo con todos los elementos que debe contener el riesgo identificado:

Figura 3 - Estructura y ejemplo para definir el riesgo de corrupción y LAFT

MATRIZ: DEFINICIÓN DEL RIESGO DE CORRUPCIÓN				
Descripción del riesgo	**Acción u omisión**	**Uso del poder**	**Desviar la gestión de lo público**	**Beneficio privado**
Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.	X	X	X	X

Fuente: Secretaría de Transparencia de la Presidencia de la República.

- **Riesgos de Seguridad de la Información:**

Para la identificación de los riesgos de seguridad de la información el proceso debe realizar inicialmente la identificación de activos acorde con los lineamientos establecidos en la metodología de clasificación y valoración de activos de información OSTI-GU01. Paso seguido deberá identificar la relación de vulnerabilidades y amenazas que pueden llegar a afectar **la integridad, disponibilidad** o **confidencialidad** del activo de información. De conformidad con la siguiente tabla:

Tabla 4 - Vulnerabilidades y amenazas para identificar riesgos de seguridad de la información

Tipo de activo	Vulnerabilidades	Amenazas	Aplica a
Información	Desconocimiento o no aplicación de las políticas de seguridad y privacidad de la información	Fallas humanas	Todos los procesos
	Manejo manual de la información	Fallas humanas	
	Ausencia de validación de autenticación de la información	Fallas humanas	
	Ausencia de copias de respaldo o backups de la información	Pérdida de información	

Tipo de activo	Vulnerabilidades	Amenazas	Aplica a
	Retraso en la salida de información de los sistemas	Falla en los sistemas	
	Retraso en la entrega de información por parte del personal	Fallas humanas	
	Información sensible sin cifrado	Hurto de información Pérdida de información	
	Ausencia o deficiencia en los sistemas de autenticación de los aplicativos	Hurto de información Pérdida de información	
	Deficiencia en la autorización de permisos de acceso a la información / Falta de controles de acceso físico.	Hurto de información Pérdida de información Modificación no autorizada	
Hardware (Equipos y Redes de Comunicación)	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento	Incumplimiento en el mantenimiento del sistema de información	Todos los procesos
	Ausencia de esquemas de reemplazo periódico	Destrucción de equipos o de medios	
	Susceptibilidad a la humedad, el polvo y la suciedad	Polvo, corrosión, congelamiento	
	Sensibilidad a la radiación electromagnética	Radiación electromagnética	Procesos de Tecnología de Información
	Ausencia de un eficiente control de cambios en la configuración	Error en el uso	
	Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía	
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos	Todos los procesos
	Almacenamiento sin protección	Hurto de medios o documentos	
	Falta de cuidado en la disposición final	Hurto de medios o documentos	
	Copia no controlada	Hurto de medios o documentos	
	Ausencia de pruebas de envío o recepción de mensajes	Negociación de acciones	
	Líneas de comunicación sin protección	Escucha encubierta	Procesos de Tecnología de Información
	Tráfico sensible sin protección	Escucha encubierta	
	Conexión deficiente de los cables	Falla del equipo de telecomunicaciones	
	Punto único de falla	Falla del equipo de telecomunicaciones	
	Ausencia de identificación y autenticación de emisor y receptor	Falsificación de derechos	
	Arquitectura insegura de la red	Espionaje remoto	
	Transferencia de contraseñas en claro	Espionaje remoto	
	Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)	Saturación del sistema de información	

Tipo de activo	Vulnerabilidades	Amenazas	Aplica a
	Conexiones de red pública sin protección	Uso no autorizado del equipo	
Software	Ausencia de terminación de la sesión cuando se abandona la estación de trabajo	Abuso de los derechos	Todos los procesos
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software	
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos	
	Falla en la producción de informes de gestión	Uso no autorizado del equipo	
	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos	Procesos de Tecnología de Información
	Defectos bien conocidos en el software	Abuso de los derechos	
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los derechos	
	Ausencia de pistas de auditoría	Abuso de los derechos	
	Asignación errada de los derechos de acceso	Abuso de los derechos	
	Software ampliamente distribuido	Corrupción de datos	
	En términos de tiempo utilización de datos errados en los programas de aplicación	Corrupción de datos	
	Interfaz de usuario compleja	Error en el uso	
	Ausencia de documentación	Error en el uso	
	Configuración incorrecta de parámetros	Error en el uso	
	Fechas incorrectas	Error en el uso	
	Ausencia de mecanismos de identificación y autenticación, como la autenticación de usuario	Falsificación de derechos	
	Tablas de contraseñas sin protección	Falsificación de derechos	
	Gestión deficiente de las contraseñas	Falsificación de derechos	
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos	
	Software nuevo o inmaduro	Mal funcionamiento del software	
	Ausencia de control de cambios eficaz	Mal funcionamiento del software	
	Descarga y usos no controlados de software	Manipulación con software	
	Ausencia de copias de respaldo	Manipulación con software	
Recurso Humano	Ausencia del personal	Incumplimiento en la disciplina del personal	Todos los procesos

Tipo de activo	Vulnerabilidades	Amenazas	Aplica a
	Procedimientos inadecuados de contratación	Destrucción de equipos o medios	
	Entrenamiento insuficiente en seguridad	Error en el uso	
	Uso incorrecto de software y hardware	Error en el uso	
	Falla de conciencia acerca de la seguridad	Error en el uso	
	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de datos	
	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos	
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo	
Infraestructura Física	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Destrucción de equipo o medios	Procesos de Gestión Administrativa
	Ubicación en un área susceptible de inundación	Inundación	
	Red energética Inestable	Pérdida del suministro de energía	
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de equipo	
Organización	Ausencia de procedimiento formal para el registro y retiro de usuarios	Abuso de los derechos	Todos los procesos
	Ausencia de proceso formal para la revisión de los derechos de acceso	Abuso de los derechos	
	Ausencia de disposición en los contratos con clientes o terceras partes (con respecto a la seguridad)	Abuso de los derechos	
	Ausencia de procedimientos de monitoreo de los recursos de procesamiento de la información	Abuso de los derechos	
	Ausencia de auditorias	Abuso de los derechos	
	Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos	
	Ausencia de reportes de fallas en los registros de administradores y operadores	Abuso de los derechos	
	Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información	
	Ausencia de acuerdos de nivel de servicio o insuficiencia de los mismos	Incumplimiento en el mantenimiento del sistema de información	

Tipo de activo	Vulnerabilidades	Amenazas	Aplica a
	Ausencia de procedimientos de control de cambios	Incumplimiento en el mantenimiento del sistema de información	
	Ausencia de procedimiento formal para la documentación del MSPI	Corrupción de datos	
	Ausencia de procedimiento formal para la supervisión del registro del MSPI	Corrupción de datos	
	Ausencia de procedimiento formal para la autorización de la información disponible al público	Datos provenientes de fuentes no confiables	
	Ausencia de asignación adecuada de responsabilidades en seguridad de la información	Negación de acciones	
	Ausencia de planes de continuidad	Falla del equipo	
	Ausencia de políticas sobre el uso de correo electrónico	Error en el uso	
	Ausencia de procedimientos para introducción del software en los sistemas operativos	Error en el uso	
	Ausencia de registros en bitácoras	Error en el uso	
	Ausencia de procedimientos para el manejo de información clasificada	Error en el uso	
	Ausencia de responsabilidad en seguridad de la información en la descripción de los cargos	Error en el uso	
	Ausencia de los procesos disciplinarios definidos en caso de incidentes de seguridad de la información	Hurto de equipo	
	Ausencia de política formal sobre la utilización de computadores portátiles	Hurto de equipo	
	Ausencia de control de los activos que se encuentran fuera de las instalaciones	Hurto de equipo	
	Ausencia de política sobre limpieza de escritorio y pantalla	Hurto de medios o documentos	
	Ausencia de autorización de los recursos de procesamiento de información	Hurto de medios o documentos	
	Ausencia de mecanismos de monitoreo establecidos para las brechas en seguridad	Hurto de medios o documentos	
	Ausencia de revisiones regulares por parte de la gerencia	Hurto de medios o documentos	
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad	Uso no autorizado de equipo	

Tipo de activo	Vulnerabilidades	Amenazas	Aplica a
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	Uso de software falsificado o copiado	

Fuente: Información tomada de guía de vulnerabilidades y amenazas del Ministerio de las Tecnologías de la Información y las Comunicaciones

Teniendo en cuenta lo anterior, en la siguiente tabla se describe la estructura para la definición de un riesgo de seguridad de la información, los cuales están relacionados con la afectación de la confidencialidad, integridad y disponibilidad de la información y sus activos asociados:

Tabla 5 - Estructura para definir el riesgo Seguridad de la Información

Área de impacto	De acuerdo con el análisis, podrá incluir en la redacción el área de impacto, ya sea por afectación económica o reputacional y considerando, además, la criticidad del activo de información.
Pilar de la información	Pérdida de la integridad
Activo	Base de datos del sistema de nómina
Amenaza	Por modificaciones no autorizadas
Causas / Vulnerabilidad (asociadas a la amenaza identificada. Tabla 4)	Debido a la deficiencia en la autorización de permisos de acceso a la información y en la ejecución de políticas de seguridad digital.
Riesgo	Posibilidad de afectación económica por pérdida de integridad de la base de datos del sistema de nómina por modificaciones no autorizadas, debido a la deficiencia en la autorización de permisos de acceso a la información y ejecución de políticas de seguridad de la información.

Fuente: Elaboración OAPCR y DGTIC

- **Elementos para complementar la etapa de identificación**

Una vez identificado el evento de riesgo se debe completar la etapa con los siguientes elementos:

a. **Descripción del riesgo:** se realiza una explicación de las características generales que se observan en el riesgo identificado, facilitando su comprensión. Dicha explicación debe responder a ¿qué puede suceder?, ¿cómo puede suceder?, ¿cuándo puede suceder?, ¿qué consecuencias tendría su materialización?

b. **Responsable:** funcionario líder de la gestión del riesgo identificado.

c. **Gestor:** funcionario responsable de la ejecución las actividades de control y de fortalecimiento del riesgo.

d. **Causas:** son las circunstancias generales, elementos o causas de carácter endógeno a la entidad o exógeno, que pueden obstaculizar el cumplimiento de su misión, visión y objetivos, o generar prácticas corruptas. Son internas atribuidas a personas, métodos, equipos, materiales e instalaciones, directamente involucradas en el proceso o procedimiento, o externas cuando provienen del entorno en el que se desarrolla. Las causas se identifican teniendo en cuenta los siguientes agentes generadores definidos:

- **Procesos:** eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.
- **Talento Humano:** incluye Seguridad y Salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.
- **Tecnología:** eventos relacionados con la infraestructura tecnológica de la entidad.
- **Infraestructura:** eventos relacionados con la infraestructura física de la entidad.
- **Evento Externo:** situaciones externas que afectan la entidad.

e. **Efectos:** son los efectos asociados a la posible materialización del riesgo operativo y de seguridad de la información, que inciden sobre los objetivos, los procesos, la entidad o país. Estos, por lo general están asociados al área de impacto.

- **Afectación económica:** representadas en multas o sanciones detrimento del patrimonio, sobre costos e inactividad, entre otras.
- **Afectación reputacional:** constituido por la pérdida de credibilidad, transparencia, confianza en el cumplimiento de la misión y tareas encomendadas; probidad en las instituciones del estado.
- **Afectación económica y reputacional:** su materialización tiene un impacto económico y reputacional.

f. **Clase de riesgos:** permite agrupar los riesgos identificados, se clasifica cada uno de los riesgos en las siguientes categorías:

- **Ejecución y Administración de Procesos:** Pérdidas derivadas de errores en la ejecución y administración de procesos.
- **Fraude Externo:** pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
- **Fraude Interno:** Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad, en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
- **Fallas Tecnológicas:** Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.
- **Relaciones Laborales:** Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
- **Usuarios, Productos y Prácticas Organizacionales:** Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
- **Daños a Activos Físicos/ Eventos externos:** Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos como atentados, vandalismo, orden público.

- **Corrupción:** Posibles actos de corrupción descritos como la probabilidad de ocurrencia de eventos en los que se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- **Estratégicos:** Afectación económica o reputacional por el incumplimiento de objetivos y metas estratégicas.
- **Lavado de Activos y Financiación del Terrorismo:** Posibilidad de pérdida o daño que podría sufrir la entidad al ser utilizada directamente o a través de sus operaciones como instrumento para el lavado de activos y/o canalización de recursos hacia la realización de actividades terroristas.
- **Conflicto de Interés:** Posibles actos o decisiones en los que el interés general propio de la función pública entró en conflicto con el interés particular y directo del servidor público, lo cual puede derivar en eventos de corrupción.
- **Opacidad:** Asociados a las deficiencias de calidad de la información que se publica como parte del derecho al acceso a información pública y de los ejercicios de rendición de cuentas. Situaciones que impidan el cumplimiento de la Ley de Transparencia.
- **Continuidad de Negocio:** Eventos que pueden comprometer la normalidad de la operación de la entidad para el cumplimiento de sus funciones.

De acuerdo con el análisis del proceso y del contexto de la entidad, esta clasificación de riesgo puede estar asociada o relacionada con los subsistemas de gestión de riesgos operativos, de corrupción LA/FT y de seguridad de la información.

g. **Otros procesos del SIGI afectados:** se especifican los procesos que se podrían ver afectados con la materialización del riesgo.

h. **Trámites u OPAS afectados:** se especifica el trámite (corresponde a los registrados en el Sistema Único de Información de Trámites-SUIT de la Función Pública) y/o OPA posiblemente afectados con la materialización del riesgo.

- **Riesgos de contratación:**

Los riesgos relacionados con los contratos suscritos por la ADRES, en todo el ciclo de la gestión contractual, se identifican y administran conforme a lo establecido en el Manual de Contratación y la normativa vigente sobre la materia.

7.3 ANÁLISIS DEL RIESGO

Esta etapa busca establecer la probabilidad de ocurrencia del riesgo y las consecuencias o impacto que puede generar su eventual materialización, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE).

Para riesgos operativos, de crédito, de mercado, de liquidez o de seguridad de la información se utiliza una matriz de valoración de 5 filas por 5 columnas, mientras que para riesgos de corrupción y de LAFT la correspondiente a 5 filas por 3 columnas.

Figura 4 - Mapa de calor para riesgos operativos de crédito, de mercado, de liquidez y de seguridad de la información.

		Impacto				
		Insignificante	Menor	Moderado	Mayor	Catastrófico
Probabilidad	Muy Alta	Alto	Alto	Alto	Alto	Extremo
	Alta	Moderado	Moderado	Alto	Alto	Extremo
	Media	Moderado	Moderado	Moderado	Alto	Extremo
	Baja	Bajo	Moderado	Moderado	Alto	Extremo
	Muy Baja	Bajo	Bajo	Moderado	Alto	Extremo

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas (DAFP) - Versión 6

Figura 5 - Mapa de calor para riesgos de corrupción y LAFT

		Impacto		
		Moderado	Mayor	Catastrófico
Probabilidad	Casi seguro	Extremo	Extremo	Extremo
	Probable	Alto	Extremo	Extremo
	Posible	Alto	Extremo	Extremo
	Improbable	Moderado	Alto	Extremo
	Rara vez	Moderado	Alto	Extremo

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas (DAFP) - Versión 6

El riesgo inherente se obtiene del cruce del resultado de la probabilidad y del impacto de acuerdo con las siguientes consideraciones:

7.3.1 Determinar la probabilidad de ocurrencia

- **Criterios para calificar la probabilidad – riesgo de gestión, corrupción, seguridad de la información**

La probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De esta forma la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año, es decir, la frecuencia en que se ejecuta la actividad.

Tabla 6 - Criterios para definir probabilidad

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta máximo 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces al año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año.	100%

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, Versión 6.

Para los riesgos de corrupción, en la probabilidad se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de frecuencia o factibilidad, donde la frecuencia implica analizar el número de eventos de un periodo determinado, se trate de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; implica analizar la presencia de factores externos e internos que pueden propiciar el riesgo, de un hecho que no se ha presentado, pero es posible que suceda.

Tabla 7 - Encuesta para determinar el impacto en riesgos de corrupción y LAFT

Nivel	Descriptor	Descripción	Frecuencia
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año
3	Posible	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
2	Improbable	El evento puede ocurrir en algún momento	Al menos 1 vez en los últimos 5 años
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales)	No se ha presentado en los últimos 5 años

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, Versión 6Determinar consecuencias o nivel de impacto

7.3.2 Determinar consecuencias o nivel de impacto

- **Criterios para calificar el impacto – riesgo de corrupción y LAFT**

En riesgos de corrupción se diligencia el siguiente cuestionario definido por la Guía para la Gestión del Riesgos de Corrupción de la Secretaría de Transparencia de la Presidencia de la República.

Tabla 8 - Encuesta para determinar el impacto en riesgos de corrupción y LAFT.

Encuesta para determinar el impacto del riesgo		Respuesta	
No	**Pregunta: si el riesgo se materializa podría...**	**Si**	**No**
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectas el cumplimiento de la misión de la Entidad?		
4	¿Afectar el cumplimiento de la misión del Sector Salud y Protección Social?		
5	¿Generar pérdida de confianza de la Entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicios o los recursos públicos?		
9	¿Generar pérdida de la información de la Entidad?		
10	¿Generar intervención de los Órganos de Control, de la Fiscalía, u otro ente?		
11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		
14	¿Dar lugar a procesos penales?		
15	¿Generar pérdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		

Fuente: Guía para la Gestión de Riesgos de Corrupción, Presidencia de la República, 2015

El impacto en riesgos de corrupción se obtiene de acuerdo con las respuestas obtenidas, cuya escala es la siguiente:

Tabla 9 - Escala de impacto con enfoque de corrupción y LAFT.

Nivel	Escala	Descripción	Respuestas afirmativas
1	Moderado	Genera medianas consecuencias sobre la entidad.	1 a 5
2	Mayor	Genera altas consecuencias sobre la entidad.	6 a 11
3	Catastrófico	Genera consecuencias desastrosas para la entidad.	12 a 19

Criterios para calificar el impacto – Riesgos operativos, de seguridad de la información, de crédito, mercado y liquidez.

Para determinar el impacto se tiene en cuenta la siguiente tabla, considerando la afectación reputacional y económica.

Figura 6 - Calificación del Impacto – Riesgos operativos, de seguridad de la información, de crédito, liquidez, mercado y de seguridad de la información.

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	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.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	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.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas (DAFP) - Versión 6.

Para los riesgos de seguridad de la información se debe tener en cuenta la criticidad que se defina del activo en el Matriz de identificación de activos de información, la cual es una guía sugerida para la identificación del impacto y será responsabilidad del líder del proceso validarla, teniendo en cuenta lo siguiente:

Tabla 10 - Convalidación de impacto según criticidad de activos de información

Criticidad del activo	Calificación de impacto
Bajo	Insignificante
	Menor
Medio	Moderado
	Mayor
Alto	Catastrófico

7.4 VALORACIÓN DE CONTROLES

Los controles corresponden a herramientas o prácticas que se disponen en la actualidad para reducir la probabilidad de ocurrencia (preventivos o detectivos) o el impacto (correctivos) que pueda generar la materialización del riesgo, deben establecerse y redactarse en términos de actividad y redactarse para cada riesgo.

Una adecuada redacción de control debe contener en su estructura los siguientes elementos;

- **Responsable de ejecutar el control:** identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.
- **Acción:** se determina mediante verbos que indican la acción que deben realizar como parte del control.
- **Complemento:** detalles que permitan identificar el objeto del control.

A través del ciclo de procesos y la forma como se ejecutan, es posible establecer cuándo se activa un control y, por tanto, establecer una tipología con precisión, como se resume en la siguiente tabla.

Tabla 11 - Atributos para el diseño del control.

Características de Eficiencia		Peso	Definición
Tipo	Preventivo	25%	Acción y/o mecanismo ejecutado en la entrada del proceso antes de que se realice la actividad originadora del riesgo, que busca establecer condiciones que aseguren el resultado final esperado. En general estos controles actúan sobre las causas del riesgo.
	Detectivo	15%	Acción y/o mecanismo ejecutado durante la ejecución del proceso. Estos controles detectan el riesgo, pero genera reprocesos.
	Correctivo	10%	Acción que se ejecuta en la salida del proceso y después de que se materializa el riesgo y en la mayoría de las ocasiones permiten reducir el impacto de dicho riesgo. Estos controles tienen costos implícitos.
Implementación	Automático	25%	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática.
	Manual	15%	Controles que son ejecutados por una persona, tiene implícito el error humano.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas (DAFP) - Versión 6

Adicional a los atributos anteriores, se debe tener en cuenta los atributos informativos que permiten darle formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos; éstos no tienen una incidencia directa en su efectividad.

Tabla 12 - Atributos informativos para formalización del control.

Formalización del Control		Definición
Documentación	Documentado	Identifica los controles que están documentados en el proceso, ya sea en manuales, procedimientos o cualquier otro documento propio del proceso. Los puntos de control documentados deben contener una adecuada segregación de funciones.
	Sin Documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso
Frecuencia	Continua	Este atributo identifica a los controles que se ejecutan siempre que se realiza la actividad originadora del riesgo.

Formalización del Control		Definición
	Aleatoria	Este atributo identifica a los controles que no siempre se ejecutan cuando se realiza la actividad originadora del riesgo.
Evidencia	Con registro	El control deja un registro, permite evidenciar la ejecución del control.
	Sin registro	Son aquellos controles que se ejecutan, pero no dejan ningún tipo de evidencia de su ejecución

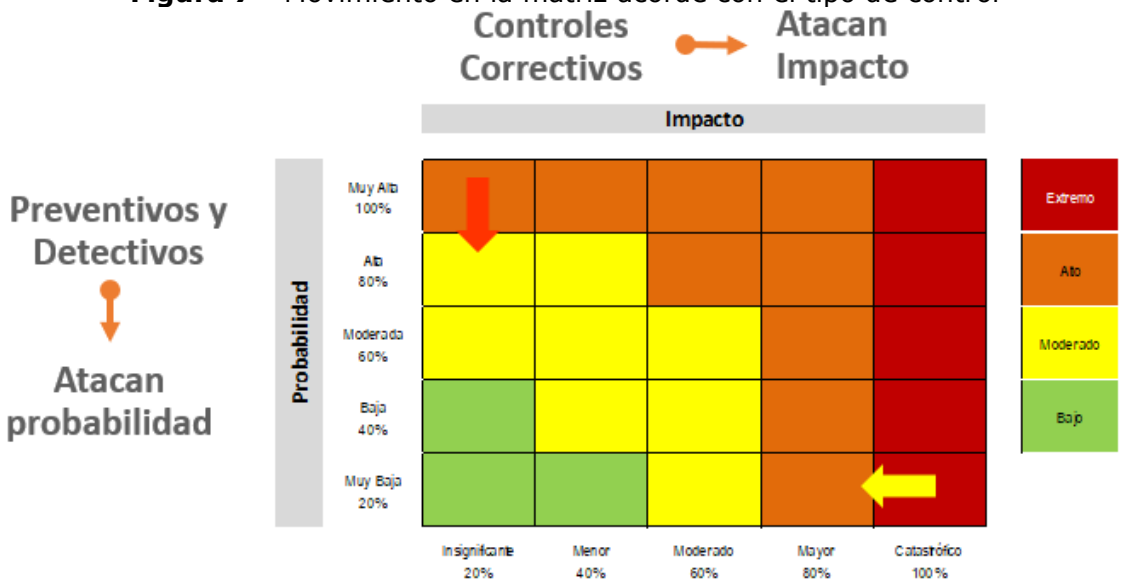
Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas (DAFP) - Versión 6

Nota: La existencia de controles frente a la probabilidad o impacto dependerá del escenario de riesgo en particular.

- **Desplazamiento en la Matriz – Riesgo Residual**

El resultado de aplicar la efectividad de los controles al riesgo inherente permite determinar el riesgo residual. Se identifica si los controles reducen la probabilidad o el impacto, para así reducir porcentualmente cada variable.

Figura 7 - Movimiento en la matriz acorde con el tipo de control



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas (DAFP) - Versión 6

A partir de los controles que se identifiquen para la gestión de cada riesgo analizado, los controles preventivos y detectivos, reducirán la probabilidad de ocurrencia del evento, en tanto que los controles correctivos reducirán los impactos de este. Producto de este análisis se obtiene el nivel residual del riesgo.

7.5 MANEJO DEL RIESGO

La etapa de manejo se enfoca en la decisión que se toma frente a un determinado nivel de riesgo, dicha decisión puede ser aceptar, reducir, compartir o evitar. Se analiza frente a riesgo residual para los procesos en funcionamiento, para los nuevos, se produce a partir del riesgo inherente.

- **Opciones de manejo**

Una vez se ha determinado el riesgo residual, se debe asociar la opción de manejo mediante la cual se dará tratamiento. Las opciones de manejo se determinan teniendo en cuenta la ubicación del riesgo según las zonas definidas así:

Tabla 13 - Opciones de manejo del riesgo.

Zona de Riesgo	Operativos	Corrupción y LAFT	Crédito, Mercado y Liquidez	Seguridad de la información
Baja	Aceptar Reducir Evitar	No aplica	Aceptar Reducir Evitar	Aceptar Reducir Evitar
Moderada	Aceptar Reducir Evitar	Reducir Evitar Compartir	Reducir Evitar	Aceptar Reducir Evitar
Alta	Reducir Evitar	Reducir Evitar Compartir	Reducir Evitar	Reducir Evitar
Extrema	Reducir Evitar	Reducir Evitar Compartir	Reducir Evitar	Reducir Evitar

- **Aceptar el riesgo:** aceptar o asumir la pérdida residual probable, conociendo los efectos de su posible materialización, en este tratamiento deberán definirse las posibles acciones de contingencia para su manejo. Esta opción es la más viable para los riesgos valorados como "bajo"; sin embargo, puede existir otros a los que no se les puede aplicar controles adicionales y por lo tanto se acepta el riesgo. Aunque se adopte esta opción, el líder del proceso debe hacer seguimiento continuo al riesgo. Ningún riesgo de corrupción podrá ser aceptado.

- **Reducir el riesgo:** implica realizar un análisis y considerar, dependiendo del nivel del riesgo, si se determina tratarlo mediante transferencia o mitigación, y formular acciones o medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección), las cuales se incluyen como acciones de fortalecimiento para el riesgo. Lo anterior, cuando el nivel del riesgo se ubica en zona moderada, alta o extrema. Ej.: optimización de procesos, definición de nuevos controles, capacitaciones, entre otros.
  - Transferir: después de analizar el riesgo se determina tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas. La responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputacional.
  - Mitigar: después de un análisis y considerar los niveles de riesgo, se implementan acciones que mitiguen el nivel de riesgo. No necesariamente es un control adicional.

Para riesgos de corrupción se adoptarán medidas para reducir la probabilidad o el impacto del riesgo, o ambos, lo cual puede conllevar a implementar controles. En este caso deberán seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el riesgo logre la reducción esperada.

- **Evitar el riesgo:** tomar las medidas encaminadas a NO asumir la actividad que genera este riesgo, es decir, no iniciar o no continuar con la actividad que provoca el riesgo.

- **Compartir el riesgo:** Aplicable a riesgos de corrupción. Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad.

➢ Acciones de fortalecimiento a la gestión del riesgo

Como resultado de la valoración de los controles y de la opción de manejo definida se formulan las acciones orientadas al mejoramiento y fortalecimiento de la gestión del riesgo; estas acciones deben establecer un responsable y una fecha específica y son obligatorias cuando:

- Se identifican fallas en los controles existentes.
- Se define como opción de manejo evitar o reducir riesgo, esto dependiendo la zona de riesgo residual.

Cuando todos los controles asociados al riesgo tienen una calificación positiva en los criterios de evaluación, no es necesaria la formulación de acciones adicionales.

Nota 1: las posibles acciones a emprender deben ser viables en su ejecución y tener relación con el riesgo identificado.
Nota 2: las acciones que se definan como nuevas no deben ser los mismos controles ya establecidos.
Nota 3: las acciones frente al riesgo con enfoque de control tienen una connotación preventiva.

➢ Indicadores clave de riesgo

Durante esta etapa se identifican los indicadores que estarán asociados a eventos o incidentes cuyo comportamiento puede indicar mayor o menor exposición al riesgo identificado. Para poderlos relacionar, estos deben estar formulados y aprobados en el módulo de indicadores de Eureka. No es obligatorio construir indicadores para todos los riesgos identificados, sin embargo, se consideran elementos importantes, pues permiten llevar un registro de ocurrencias y evaluar a través de su tendencia la eficacia de los controles que se disponen para mitigar los riesgos previamente definidos.

Los indicadores clave de riesgo, deben ser diferentes a los indicadores de proceso.

➢ Acciones de Contingencia frente al riesgo

Es necesaria la formulación de acciones de contingencia, toda vez que existe una mínima posibilidad de que el riesgo se presente. Las actividades que se definan, en la medida de lo posible, deben permitir el normal desarrollo del proceso o la gestión de la Entidad ante la materialización de un riesgo.

Nota 1: las posibles acciones a emprender deben ser viables en su ejecución y tener relación con el riesgo identificado.
Nota 2: las acciones frente al riesgo con enfoque de contingencia tienen una connotación correctiva.

8 REVISIÓN Y APROBACIÓN

La aprobación de los riesgos es realizada por el (los) cargos responsables de gestionar cada uno de los riesgos identificados, siendo el líder del proceso o procedimiento respectivo. Esto a través del flujo de Solicitudes del SIGI, en el módulo de mejoras de Eureka.

Aspectos para tener en cuenta:

- La fecha de aprobación de cada riesgo documentado corresponde a la fecha de aprobación del líder del proceso en Eureka.
- Cualquier modificación a los riesgos y a las acciones de fortalecimiento formuladas debe ser tramitada por Eureka, con el acompañamiento de los asesores de la Oficina Asesora de Planeación y Control de Riesgos, a través del flujo de Solicitudes del SIGI, en el módulo de mejoras de Eureka.

- **Revisión metodológica**

El Equipo de la Oficina Asesora de Planeación y Control de Riesgos (en riesgos operativos y corrupción y LAFT), la Dirección de Gestión de Tecnologías de Información y Comunicaciones (en riesgos de seguridad de la información) y la Dirección de Recursos Financieros de la Salud (en riesgos de crédito, liquidez y mercado), revisan entre otros, los siguientes aspectos metodológicos durante la construcción de las fichas de riesgos:

1. Consistencia entre el contenido de los riesgos diligenciadas y el objetivo del proceso o estratégico.
2. Existencia de los documentos como resultado de la gestión de riesgos.
3. Coherencia en la definición de acciones frente a los controles o de contingencia y
4. Aplicación de las disposiciones definidas en el presente Manual.
5.

9 MAPA INTEGRAL DE RIESGOS DEL PROCESO

El mapa integral de riesgos del proceso consolida la información de todos los riesgos de la entidad para los enfoques operativo, corrupción y LAFT, crédito, liquidez y mercado, en caso de contenerlos.

La fecha del mapa de riesgos del proceso corresponde a la fecha de aprobación más reciente entre el conjunto de los riesgos.

10 MAPA DE RIESGOS INSTITUCIONAL

Contiene los riesgos identificados y aprobados en los procesos de la entidad (operativo, corrupción y LAFT, seguridad de la información, crédito, liquidez y mercado), permitiendo conocer la aplicación

de las opciones de tratamiento. Este documento se actualiza de acuerdo con la dinámica de riesgos al interior de la Entidad.

11 COMUNICACIÓN Y CONSULTA

Acción transversal donde el proceso debe hacer partícipe a sus colaboradores en las diferentes etapas y asegurar la consulta y conocimiento de los riesgos, controles y acciones establecidas.

El mapa de riesgos actualizado y consolidado es publicado en la página web antes del 31 de enero de cada vigencia.

12 INFORMACIÓN, COMUNICACIÓN Y REPORTE

Acciones de la primera línea de defensa:

- El líder del proceso deberá realizar la revisión y aprobación de la documentación del proceso relacionada con la gestión de riesgos.
- El responsable de la gestión del riesgo es quién reporta la materialización del riesgo, así como la formulación del plan de mejoramiento.
- El responsable de la gestión del riesgo debe enviar al correo electrónico gestionderiesgos@adres.gov.co el reporte de conocimiento de operaciones sospechosas en caso de que este se presente.
- El líder del proceso y/o el profesional que este designe deberá reportar mediante la herramienta establecida para la gestión de riesgos, el reporte de avance de las acciones y controles de mitigación de riesgos, (con fechas límites de reporte (30 de abril, 31 de agosto, 31 de diciembre en caso de que estos días sean festivos o fines de semana el reporte se deberá hacer a más tardar el día hábil anterior).

Acciones de la segunda línea de defensa:

- La Oficina Asesora de Planeación y Control de Riesgos deberá consolidar el mapa de riesgos institucional y gestionar su respectiva publicación y actualización cada vez que se requiera, como mínimo una vez en la vigencia.
- La Oficina Asesora de Planeación y Control de Riesgos deberá elaborar, cuatrimestralmente, el informe de seguimiento a la gestión de riesgos
- La Oficina Asesora de Planeación y Control de Riesgos deberá realizar el seguimiento a los planes de mejoramiento por concepto de eventos de riesgos materializados.

Acciones de la tercera línea de defensa:

La Oficina de Control Interno debe gestionar la publicación del informe de seguimiento generado en la página Web de la ADRES.

13 MONITOREO Y REVISIÓN

El líder del proceso debe realizar cuatrimestralmente el reporte de monitoreo y revisión de la gestión de los riesgos del proceso lo cual incluye determinar:

- El nivel de ejecución de las acciones de fortalecimiento a la gestión del riesgo.
- Si los controles establecidos se encuentran operando con normalidad.
- Si se han generado alertas tempranas.
- Si el riesgo se ha materializado (reporte que debe ser realizado en Eureka con el correspondiente plan de mejora)
- Identificación de nuevos riesgos

La Oficina Asesora de Planeación y Control de Riesgos cada cuatrimestre realiza la revisión del monitoreo al reporte de seguimiento a la gestión de riesgos que realiza la primera línea de defensa.

Los riesgos estratégicos serán monitoreados mínimo una vez al año, en el marco del seguimiento al Plan Estratégico Institucional.

14 SEGUIMIENTO Y EVALUACIÓN

La Oficina de Control Interno realiza el seguimiento y evaluación, cuya finalidad es sugerir los correctivos y ajustes necesarios que permitan un adecuado tratamiento del riesgo, propendiendo por la formulación de planes de mejoramiento y tratamiento a las situaciones detectadas.

La evaluación adelantada por la Oficina de Control Interno a la administración de riesgos involucra los siguientes aspectos entre otros:

- Ajustes en el análisis o valoración de los riesgos identificados, producto del seguimiento y calificación a los controles establecidos, y los cambios presentados en cuanto a la probabilidad e impacto.
- Verificación de la ejecución del procedimiento Administración de Riesgos DIES-PR02.
- Verificar que los controles definidos para tratar los riesgos existen, funcionan y son suficientes.
- Verificar la operatividad –ejecución- de los controles identificados en el mapa de riesgos.
- Validar la operatividad –ejecución- de las acciones de tratamiento de riesgos definidas.
- Verificar que el tratamiento de los riesgos es adecuado y efectivo.
- Verificar la implementación de la Política de Administración de Riesgos.
- Verificar las evidencias de la revisión del mapa de riesgos del proceso.
- Verificar que los responsables de los riesgos adelanten acciones para la identificación de riesgos y se revisen periódicamente.
- Verificar la aplicación acciones de fortalecimiento a la gestión de riesgos.

15 ACCIONES FRENTE A LA MATERIALIZACIÓN DE RIESGOS

En el evento de materializarse un riesgo, el enlace del proceso debe generar el reporte de en Eureka, diligenciado lo siguiente:

- Fecha de materialización
- Descripción del evento
- ¿Que causó la posible materialización del riesgo?
- Documentos del SIGI relacionados (asociar los procedimientos que contienen los puntos de control que no fueron efectivos)
- ¿Qué control no fue efectivo para evitar la materialización del riesgo?
- ¿Qué impacto genera para el proceso o la institución la materialización de ese riesgo?
- ¿Es posible que se haya presentado en otras ocasiones sin haberlo detectado?
- ¿Qué acciones se deben realizar para reestablecer el curso de acción del proceso?
- ¿Qué actividades se deben desarrollar para fortalecer los controles?
- ¿Cuáles procesos están implicados en la materialización del riesgo?
- Plan de mejora relacionado, el cual se debe crear en el módulo de mejoras en Eureka, como una acción correctiva, según lo definido en GEDO-PR03 Formulación Seguimiento Planes de Mejoramiento.

Cuatrimestralmente el gestor de operaciones de la Oficina Asesora de Planeación y Control de Riesgo realiza seguimiento a las materializaciones registradas con el propósito de revisar avances y verificar que el plan establecido se esté ejecutando de acuerdo con lo planeado y aprobado por el líder del proceso. De requerir alcances o ajustes en los planes en ejecución, se informa al enlace del proceso. El seguimiento realizado por la OAPCR queda registrado en el informe de gestión de riesgos.

Es responsabilidad del líder de proceso y su equipo de trabajo realizar el seguimiento oportuno y de calidad a las tareas establecidas en el plan de mejoramiento suscrito. De igual forma, son responsables de realizar el monitoreo del riesgo cada dos mes, hasta que se de cierre al plan de mejora establecido.

En el evento de materializarse un riesgo de corrupción, es necesario realizar los ajustes necesarios con acciones, tales como:

- Informar a las autoridades de la ocurrencia del hecho de corrupción.
- Revisar el mapa de riesgos de corrupción, en particular, las causas, riesgos y controles.
- Verificar si se tomaron las acciones y se actualizó el mapa de riesgos de corrupción.
- Llevar a cabo un monitoreo permanente.

16 MEDICIÓN Y ANÁLISIS DE INDICADORES EN LA GESTIÓN DEL RIESGO

Se determinan como indicadores aquellos que generen alertas previo a la materialización del riesgo y deben ser reportados por vigencia a nivel de proceso, continuando con el Procedimiento GEDO-PR02 Medición de Gestión Institucional.

17 TOMA DE DECISIONES AJUSTES O MEJORA

Como resultado del análisis realizado se generarán los ajustes requeridos tanto en la metodología como en el desarrollo de las etapas establecidas a nivel de proceso y de la entidad.

18 SUBSISTEMA DE ADMINISTRACIÓN DE RIESGOS DE LAVADO DE ACTIVOS Y FINANCIACIÓN DEL TERRORISMO

El Riesgo de Lavado de Activos y Financiación del Terrorismo corresponde a la posibilidad que, en la realización de las operaciones de la ADRES, esta pueda ser utilizada por organizaciones criminales como instrumento para ocultar, manejar, invertir o aprovechar dineros, recursos y cualquier otro tipo de bienes provenientes de actividades delictivas o destinados a su financiación, o para dar apariencia de legalidad a las actividades delictivas o a las transacciones y fondos de recursos vinculados con las mismas.

Dentro de los delitos fuente del Lavado de Activos y la Financiación del Terrorismo (LA/FT) se encuentra el riesgo de corrupción y opacidad.[3]

18.1 ALCANCE Y EFECTOS DEL LAVADO DE ACTIVOS EN LA ADRES

El lavado de activos en la ADRES se vincula al riesgo legal y reputacional a que se expone una entidad, con el consecuente efecto económico negativo que ello puede representar para su estabilidad financiera, al ser utilizada para el ocultamiento, manejo, inversión o aprovechamiento, en cualquier forma, de dinero u otros bienes provenientes de actividades delictivas, o para dar apariencia de legalidad a las transacciones y fondos vinculados con las mismas.

18.2 CUESTIONARIO DE VULNERABILIDAD DE LA/FT

Con el fin de determinar cuáles son los posibles riesgos a los cuales se podría ver expuesta la ADRES en el desarrollo de sus actividades y a que procesos aplican; se tienen en cuenta todos los factores de riesgo tanto interno como externo y a través de un instrumento de validación (cuestionario), el cual se actualiza periódicamente de acuerdo con la información aportada por cada uno de los procesos de la entidad.

[3] Circular 06 de 2018 la Superintendencia Nacional de Salud

Tabla 14 - Cuestionario de LA/FT aplicado por proceso.

Cuestionario de LA/FT		
Pregunta	**Respuesta**	**Justificación**
¿El proceso realiza transacciones a través de títulos valores tales como CDT, Acciones, BOCAS y/o otros (en caso de otros, indique cuales)?		
¿El proceso incluye políticas y procedimientos para el conocimiento adecuado de cada uno de los clientes, proveedores y sus beneficiarios, mantiene actualizada la información comercial y financiera, e identifica la legitimidad de sus actividades económicas y el origen y destino de sus fondos?		
¿El proceso realiza convenios de recaudo con las entidades financieras, permitiendo acceder a la información de terceros que giran a la ADRES?		
¿El proceso realiza la creación de terceros en los sistemas de información de la ADRES?		
¿El proceso tiene injerencia en la autorización de los movimientos de las cuentas maestras de las EPS?		
¿En el proceso realizan creación de cuentas bancarias?		
¿En el proceso se manejan bases de datos o aplicativos que contengan información de clientes y/o proveedores?		
¿En el proceso se mantienen registros de las transacciones con sus clientes y/o proveedores y su información relevante, por el tiempo mínimo legal requerido?		
¿En el proceso se puede acceder a los reportes de las entidades financieras, permitiendo acceder a la información de terceros que giran a la ADRES?		
¿En el proceso se realiza alguna actividad de vinculación de personal?		
¿En el proceso se realiza algún tipo de contratación, subcontratación o participación de proveedores?		
¿En el proceso se realizan transferencias electrónicas de divisas?		
¿En el proceso se reciben y/o gestionan recursos en divisas?		

La tabla anterior, muestra el cuestionario de LA/FT, que permite identificar los proceso que pueden tener asociados riesgos de LAFT, con el propósito de priorizar procesos e identificar las actividades que en su desarrollo podrían tener relación con LA/FT, permitiendo determinar que este sistema aplica a todos los clientes o vinculados contractualmente con cualquier entidad, sea empresa privada u organismo público.

18.3 VERIFICACIÓN DE PROCESOS DE DEBIDA DILIGENCIA

La verificación se realiza en el marco de la Política de Debida Diligencia (DIES-PL02), la cual tiene por objetivo:

"Describir los lineamientos, controles y procedimientos que permiten disminuir la probabilidad de relacionamiento con servidores públicos, contratistas, proveedores o terceros beneficiarios de giros en el marco de procesos misionales que implique que ADRES pueda ser utilizada por organizaciones criminales como instrumento para ocultar, manejar, invertir o aprovechar dineros, recursos y cualquier otro tipo de bienes provenientes de actividades delictivas o destinados a su financiación, o para dar apariencia de legalidad a las actividades delictivas o a las transacciones y fondos de recursos vinculados con las mismas."

18.4 REPORTE OPERACIONES INUSUALES Y/O SOSPECHOSAS

Los líderes de proceso deben realizar análisis de operaciones inusuales en cada uno de los procesos a cargo y en caso de identificar posibles transacciones inusuales o sospechosas deben informar al Jefe de la Oficina Asesora de Planeación y Control de Riesgos.

El Jefe de la Oficina Asesora de Planeación y Control de Riesgos será el responsable de realizar los análisis y reportes de operaciones sospechosas a la UIAF, conforme a las instrucciones impartidas en los manuales y formatos contenidos en la página de internet de dicha Entidad: http://www.uiaf.gov.co/reportantes.

Las anteriores actividades se deben realizar en el marco del procedimiento DIES-PR06 Reporte de Operaciones Inusuales o Sospechosas – SARLAFT.

Consideraciones:

Una operación intentada o una operación sospechosa debe reportarse de manera inmediata como ROS directamente a la UIAF.

Los soportes de la operación reportada se deben organizar y conservar como mínimo por cinco (5) años, dado que pueden ser solicitados por las autoridades competentes.

Ninguna persona de la ADRES podrá dar a conocer que se ha efectuado el reporte de una operación sospechosa a la UIAF, según lo determina el inciso cuarto del artículo 11 de la Ley 526 de 1999.

18.5 CAPACITACIÓN SARLAFT

La ADRES realizará jornadas de capacitación y/o sensibilización como mínimo una vez al año a todo el personal, sobre políticas, procedimientos, herramientas y controles adoptados para dar cumplimiento al SARLAFT.

En los procesos de inducción y reinducción se contemplarán temas de LA/FT.

19 RIESGOS ESTRATÉGICOS

El objetivo de este capítulo es describir una metodología que permita gestionar los riesgos estratégicos identificados en el ejercicio de la definición del Plan Estratégico 2023 -2026 con el fin de disminuir la incertidumbre y eventos que puedan afectar el logro de los objetivos estratégicos de la ADRES definidos para este cuatrienio mediante la aplicación de los criterios definidos para este fin

19.1 Alcance

Gestionar los riesgos estratégicos identificados en el marco del desarrollo del plan estratégico institucional para el cuatrienio 2023 – 2024 y el cumplimiento de los objetivos estratégicos

19.2 Marco teórico y de referencia para de la definición metodológica de gestión de riesgos estratégicos

Las metodologías más utilizadas para la gestión de los riesgos Estratégicos son las siguientes:

- **Gestión de Riesgos Empresariales o Estratégicos (ERM):**

Descripción: El ERM es un enfoque integral que busca identificar y gestionar los riesgos en toda la organización, incluyendo riesgos estratégicos, operativos, financieros y de cumplimiento. Se enfoca en la alineación de la gestión de riesgos con los objetivos y la estrategia de la organización.

Proceso: El ERM suele seguir un proceso que incluye la identificación de riesgos, la evaluación y cuantificación de riesgos, la formulación de estrategias de gestión de riesgos, la implementación de controles y medidas de mitigación, y el monitoreo continuo.

- **Análisis PESTEL**:

Descripción: Este enfoque se centra en la identificación de riesgos estratégicos a través del análisis de factores políticos, económicos, sociales, tecnológicos, ambientales y legales (PESTEL, por sus siglas en inglés) que pueden afectar a la organización.

Proceso: Se analizan estos factores externos para identificar tendencias, oportunidades y amenazas que podrían influir en la estrategia de la organización.

- **Escenarios de Riesgo:**

Descripción: Los escenarios de riesgo implican la creación de situaciones hipotéticas en las que ocurren eventos de riesgo significativos. Estos escenarios ayudan a evaluar el impacto potencial de eventos específicos en los objetivos estratégicos.

Proceso: Se desarrollan escenarios de riesgo basados en suposiciones y se evalúa cómo afectarían los objetivos estratégicos.

- **Mapeo de Riesgos Estratégicos:**

Descripción: El mapeo de riesgos estratégicos implica la visualización de riesgos en un mapa estratégico. Esto ayuda a comprender cómo los riesgos pueden influir en la consecución de objetivos estratégicos.

Proceso: Se identifican riesgos estratégicos y se los representa en un mapa junto con los objetivos estratégicos relevantes.

- **Benchmarking de Riesgos:**

Descripción: El benchmarking de riesgos implica comparar la exposición al riesgo de una organización con la de sus competidores o con la industria en general.

Proceso: Se recopilan datos de riesgos de organizaciones similares para evaluar la posición de la organización en comparación con otros actores del mercado

19.3 Etapas para el desarrollo de la gestión de riesgos estratégicos

En el proceso de análisis y valoración de los riesgos se definen las siguientes etapas dentro del ciclo de gestión:

Tabla 15 – Etapas de análisis y valoración de Riesgos Estratégicos

Paso	Descripción
1. Identificación	Identificar los factores externos que pueden afectar a la organización. Estos factores suelen ser políticos (P), económicos (E), sociales (S), tecnológicos (T), ambientales (E) y legales (L).
2. Recopilación	Recopilar información relevante sobre cada uno de los factores identificados. Esto puede incluir datos, estadísticas, informes, noticias y análisis de expertos.
3. Análisis	Evaluar el impacto de cada factor en la organización. ¿Cómo pueden influir estos factores en la estrategia, operaciones, finanzas y reputación de la organización?
4. Priorización	Clasificar los factores según su importancia y probabilidad de ocurrencia. Identificar aquellos factores que tienen un impacto significativo y alta probabilidad.
5. Evaluación de Riesgos	Evaluar los riesgos asociados a cada factor identificado. Esto implica determinar la magnitud del riesgo y su probabilidad. Así como la alineación de la gestión de los riesgos internos que puedan afectar las estrategias y el objetivo estratégico asociado.
6. Desarrollo de Estrategias	Desarrollar estrategias para abordar y mitigar los riesgos identificados. Esto puede incluir cambios en la estrategia empresarial, adaptaciones operativas o medidas de contingencia.
7. Monitoreo Continuo	Establecer un proceso de monitoreo continuo de los factores PESTEL y los riesgos identificados. Mantenerse al tanto de los cambios en el entorno y ajustar las estrategias según sea necesario.

En el desarrollo de este ciclo de valoración de los riesgos se pueden identificar y gestionar proactivamente los riesgos asociados a factores externos, así como también asociarlos a los factores internos producto o resultado de la gestión integral de los subsistemas de riesgos definidos en la ADRES.

19.4 Evaluación de los Riesgos Estratégicos

La evaluación de Riesgos Estratégicos se basará en la metodología PESTEL como herramienta útil para comprender el entorno en el que opera una organización y anticipar eventos de riesgos que la afecten en el desarrollo de sus estrategias teniendo en cuenta los siguientes factores.

Factor PESTEL	Riesgos Estratég.	Evaluación de Riesgos (Impacto/Probabilidad, basada en metodología DAFP)	Estrategias de Mitigación	Responsable	Fecha de Revisión
Político	[Lista de riesgos]	[Insignificante/Menor/Moderado/ Mayor/Catastrófico] [Muy Alta/Alta/Moderada/Baja/Muy Baja]	[Descripción de estrategias]	[Nombre]	[Fecha]
Económico	[Lista de riesgos]	[Insignificante/Menor/Moderado/ Mayor/Catastrófico] - [Muy Alta/Alta/Moderada/Baja/Muy Baja]	[Descripción de estrategias]	[Nombre]	[Fecha]
Social	[Lista de riesgos]	[Insignificante/Menor/Moderado/ Mayor/Catastrófico] - [Muy Alta/Alta/Moderada/Baja/Muy Baja]	[Descripción de estrategias]	[Nombre]	[Fecha]
Tecnológico	[Lista de riesgos]	[Insignificante/Menor/Moderado/ Mayor/Catastrófico] - [Muy Alta/Alta/Moderada/Baja/Muy Baja]	[Descripción de estrategias]	[Nombre]	[Fecha]
Ambiental	[Lista de riesgos]	[Insignificante/Menor/Moderado/ Mayor/Catastrófico] - [Muy Alta/Alta/Moderada/Baja/Muy Baja]	[Descripción de estrategias]	[Nombre]	[Fecha]
Legal	[Lista de riesgos]	[Insignificante/Menor/Moderado/ Mayor/Catastrófico] - [Muy Alta/Alta/Moderada/Baja/Muy Baja]	[Descripción de estrategias]	[Nombre]	[Fecha]

NOTA: Los parámetros de calificación de impacto y probabilidad se basarán en la metodología definida para las demás tipologías de riesgos.

19.5 Capacitación

La ADRES realizará jornadas de capacitación y/o sensibilización como mínimo una vez al año a todo el personal, sobre políticas, procedimientos, herramientas y controles adoptados para la gestión de esta tipología de riesgo.

19 CONTROL DE CAMBIOS

Versión	Fecha	Descripción del cambio	Asesor del proceso
1	13 de septiembre de 2019	Primera versión del documento	Marian Helen Batista Pérez; Gestor de Operaciones OAPCR
2	14 de febrero de 2020	Se actualiza conforme al ajuste realizado en la Política de administración del riesgo, donde se especifica que las actividades del Comité de Riesgos serán asumidas por el Comité Institucional de Gestión y Desempeño. Se realiza la revisión General de la metodología y se ajusta la codificación (antes ADRI-M01) teniendo en cuenta la incorporación de la gestión de riesgos al proceso de Direccionamiento Estratégico	Andrea Catalina Cuesta Ruiz; Gestor de Operaciones OAPCR
3	24 de noviembre de 2020	Se ajusta conforme a la actualización de la política de Administración del Riesgo, teniendo en cuenta las modificaciones a la metodología del DAFP	Andrea Catalina Cuesta Ruiz; Gestor de Operaciones de la OAPCR
4	9 noviembre de 2021	Se ajusta conforme a la Versión 5 de la Guía de Administración de Riesgos y diseño de controles del DAFP (diciembre 2020) y teniendo en cuenta los documentos aprobados en el marco de la administración de riesgos de SARLAFT y se incluyen las acciones a ejecutar en caso de materialización	Olga Marcela Vargas; Asesor OAPCR
5	14 de septiembre de 2022	Se ajuste conforme a la actualización de la política de administración de riesgos aprobada por la Junta Directiva	Eliana Rodriguez Gomez Gestor de Operaciones OAPCR
6	12 de febrero de 2024	Se ajusta conforme a la actualización de la política de gestión de riesgos aprobada en 2023 y se incluyen directrices para la gestión de los riesgos estratégicos	Rodolfo Oswaldo Uribe Asesor asignado a la Oficina Asesora de Planeación y Control de Riesgos.

20 ELABORACIÓN, REVISIÓN Y APROBACIÓN

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Diana Esperanza Torres Gestor de Operaciones Oficina Asesora de Planeación y Control de Riesgos **Jaime Castro Ramírez** Gestor de Operaciones Oficina Asesora de Planeación y Control de Riesgos Fecha: 09 de febrero de 2024	**Rodolfo Oswaldo Uribe** Asesor asignado a la Oficina Asesora de Planeación y Control de Riesgos. Fecha: 12 de febrero de 2024	**Julieta Naranjo** Jefe (E) de la Oficina Asesora de Planeación y Control de Riesgos Fecha: 13 de febrero de 2024