Política de Administración de Riesgos en la Auditoría General de la República.

Oficina de Planeación

Acta N° 5 del 14 de junio de 2024
Comité Institucional de Coordinación de Control interno

Versión	Fecha de versión	Descripción del cambio.
6.0	14 de junio de 2024	Actualización respecto a los lineamientos para el análisis de riesgo fiscal de la guía para la administración del riesgo y el diseño de controles en entidades públicas versión 06 de 2022 del DAFP. Actualización de acuerdo con la Ley 2195 de 2022, en cuanto a identificación de riesgos de lavado de activos y financiación del terrorismo LAFT.

Contenido

INTRODUCCIÓN

La política de administración de riesgos de la Auditoría General de la República, se define por parte de la Alta Dirección de la entidad a través del Comité Institucional de Coordinación de Control Interno, se implementará con la participación del Comité Institucional de Gestión y Desempeño,

Esta política define los lineamientos, la metodología a utilizar en la gestión de riesgos, así como de los roles y responsabilidades de acuerdo con las líneas de defensa.

Como base para su formulación se empleó la *Guía para la administración del riesgo y el diseño de controles en entidades públicas*, versión 6, noviembre de 2022, del Departamento Administrativo de la Función Pública y se realizará la gestión de riesgos a través del procedimiento interno Administración de riesgos con código EV.120.P13.P.

De manera complementaria y articulada se dará cumplimiento a los requisitos establecidos en los sistemas de gestión y control bajo normas internacionales que adopte o deba adoptar la entidad.

La Auditoría General de la República, en esta ocasión incluye la gestión del riesgo fiscal, que de acuerdo con la Guía del DAFP "propone gestionar de manera efectiva los recursos, bienes e intereses públicos, previniendo efectos dañosos, lo cual a la vez permite mitigar la posibilidad de configuración de responsabilidades fiscales para los diferentes gestores públicos". Asimismo, se identificarán riesgos de lavado de activos y financiación del terrorismo LAFT.

DECLARACIÓN INSTITUCIONAL SOBRE EL COMPROMISO FRENTE A LA GESTIÓN DEL RIESGO.

La Auditoría General de la República asume el compromiso de administrar en forma adecuada los diferentes tipos de riesgos: de gestión, de seguridad de la información, de corrupción, lavado de activos y financiación del terrorismo, soborno, riesgos fiscales y todas aquellas modificaciones que la ley así lo exija, que puedan afectar los objetivos institucionales y por tanto la misión de la entidad. Para el efecto se garantizarán los medios necesarios, el apoyo metodológico y el compromiso institucional.

MARCO NORMATIVO

AÑO	NORMA	MATERIA
1993	Ley 87	Establece normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones.
2011	Ley 1474	Dicta normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción yla efectividad del control de la gestión pública.
2015	Ley 1753 PND.	Integra en un Sistema de Gestión, los Sistemas de Gestión de la Calidad (Ley 872 de 2003) y de Desarrollo Administrativo (Ley 489 de 1998) articulados con los Sistemas Nacional e Institucional de Control Interno.
2016	ISO 37001	Sistemas de gestión antisoborno.
2017	Decreto 1499 DAFP.	Modifica el Decreto 1083 de 2015 en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
2021	Manual DAFP	Manual Operativo del Modelo Integrado de Planeación y Gestión Consejo para la Gestión y Desempeño Institucional - versión 4 – marzo 2021
2022	Ley 2195	Adopta medidas en materia de transparencia, prevención y lucha contra la corrupción.
2022	ISO 27001	Sistema de Gestión de la seguridad de la información.
2022	Guía DAFP	Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 6 - noviembre de 2022.

POLÍTICA DE ADMINISTRACIÓN DE RIESGOS.

1. OBJETIVO

La política de administración de riesgos se define para gestionar de manera oportuna y adecuada los riesgos institucionales, con el fin de mitigar los posibles efectos sobre los objetivos institucionales, mediante la formulación de controles efectivos y acciones de mitigación para reducir la probabilidad y/o el impacto de los riesgos identificados en la entidad.

2. ALCANCE

La política será aplicable en todo nivel, a los once (11) procesos institucionales, a los planes y proyectos, de conformidad con cada tipo y clasificación de riesgo, bajo la responsabilidad de los líderes de proceso y de acuerdo con las correspondientes líneas de defensa.

3. NIVELES DE RESPONSABILIDAD Y AUTORIDAD FRENTE A LA ADMINISTRACIÓN DEL RIESGO, ACORDE CON LAS LÍNEAS DE DEFENSA.

Se definen desde las líneas de defensa y se determinan para la AGR, así:

LINEA DEDEFENSA	ROL	RESPONSABLE
LINEA ESTRATÉGICA	Define el marco general para la gestión del riesgo y el controly supervisa su cumplimiento. Someter a la aprobación del Comité Institucional de Coordinación de Control Interno - CICCI la política de administración del riesgo previamente estructurada por parte de la Oficina de Planeación, como segunda línea de defensa en la entidad. Socializar la política para su implementación al Comité de Gestión y Desempeño Institucional Hacer seguimiento para su posible actualización; y evaluar su eficacia frente a la gestión del riesgo institucional.	Comité Institucional de Coordinación de Control Interno - CICCI. Comité Institucional de Gestión y desempeño.
	Recomienda mejoras a la política de operación para laadministración del riesgo.	Comité de Gestión y Desempeño Institucional - CGDI.

LINEA DEDEFENSA	ROL	RESPONSABLE
PRIMERA LÍNEADE DEFENSA	Identifica, analiza y valora riesgos para cada procesoinstitucional. Diseña, implementa y monitorea los controles y los gestiona de manera directa. Formula plan de acción a los riesgos, (determina acciones, responsables y fechas de cumplimiento de las acciones). Orienta el desarrollo e implementación de políticas y procedimientos internos y asegura que sean compatibles con lasmetas y objetivos de la entidad. Desarrolla ejercicios de autocontrol para establecer la eficiencia,eficacia y efectividad de los controles seleccionados para eltratamiento de los riesgos identificados y los planes depreparación frente a la pérdida de continuidad de negocio. Reporta en el SIA POAS, los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos. Formula acciones de mejoramiento.	Líderes de los once (11)procesos institucionales. .
SEGUNDALÍNEA DEDEFENSA	Asegura que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende. Asesora a la línea estratégica en el análisis y definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo residual. Revisa el adecuado diseño de los controles para la mitigación delos riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para elfortalecimiento de estos.	Oficina de Planeación. Servidores de la Oficina de Planeación.

LINEA DEDEFENSA	ROL	RESPONSABLE
	Verifica que las acciones de control se diseñen conforme a los requerimientos de la metodología. Hace seguimiento al plan de acción establecido para la mitigaciónde los riesgos de los procesos. Revisa que el cargue de información en el SIA POAS esté acordecon lo aprobado por el líder del proceso. Acompaña y orienta a los líderes de procesos en la identificación, valoración y evaluación del riesgo. Socializa y publica el mapa de riesgos. Revisa las acciones y planes de mejoramiento establecidos paracada uno de los riesgos materializados, con el fin de que se tomenmedidas oportunas y eficaces para evitar en lo posible que se vuelvan a materializar y logar el cumplimiento a los objetivos. Supervisa, en coordinación con los demás responsables de estasegunda línea de defensa, que la primera línea identifique, valore, evalúe y realice el tratamiento de los riesgos, que se adopten los controles para la mitigación de los riesgos identificados y se apliquen las acciones pertinentes para reducir la probabilidad oimpacto de los riesgos. Evalúa que la gestión de los riesgos este acorde con la presente política de la entidad y que sean gestionados por la primera líneade defensa.	
	Proporciona información sobre la efectividad del Sistema deControl Interno, a través del enfoque basado en riesgos, incluida la operación de la	

LINEA DEDEFENSA	ROL	RESPONSABLE
	primera y segunda línea de defensa.	
	Monitorea la gestión de riesgo y control ejecutada por la primeralínea de defensa complementando su trabajo.	
TERCERA LÍNEADE DEFENSA	Revisa los cambios en el "Direccionamiento estratégico" o en el entorno y cómo estos pueden generar nuevos riesgos o modificarlos que ya se tienen identificados en cada uno de los procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables. Proporciona aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidadde los controles establecidos en los procesos.	Oficina de Control Interno Funcionarios de la Oficina de Control Interno Auditores Internos o quien haga sus veces
	Asesora a la primera línea de defensa de forma coordinada con la Oficina de Planeación, en la identificación de los riesgos y diseño de controles.	
	Lleva a cabo el seguimiento a los riesgos y estrategia de continuidad negocio consolidados en los mapas de riesgos y plande continuidad de conformidad con el Plan Anual de Auditorías internas y reporta los resultados al CICCI.	
	Realiza seguimiento a la implementación de mejoras sobre loslineamientos de continuidad del negocio.	
	Recomienda mejoras a la política de operación para laadministración del riesgo.	

4. METODOLOGÍA

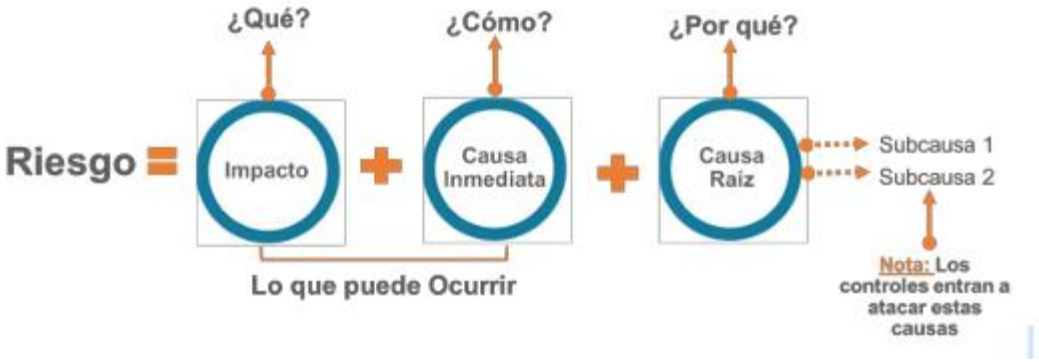
La administración de riesgos en la Auditoría General de la República, se realizará con base en la Guía de Administración de riesgos del DAFP, por medio del procedimiento interno EV.120.P13.P, y a través del Sistema de información del Sistema de Información SIA POAS, módulo "Administración de Riesgos",. Esta herramienta permite a los líderes de proceso, con el apoyo de la Oficina de Planeación, desarrollar la metodología definida. Esta metodología contempla identificar los riesgos, definir los controles, valoración y finalmente la formulación del Plan de Acción, cuando corresponda, así como el seguimiento a las acciones planeadas.

Sistema de información SIA POAS Modulo de Administración de riesgos: El sistema de información, SIA POAS facilita la gestión de los riesgos, dado que permite realizar cada etapa en una pestaña del sistema SIA, "identificación, valoración y plan de acción", lo que permite en un proceso sencillo e intuitivo.

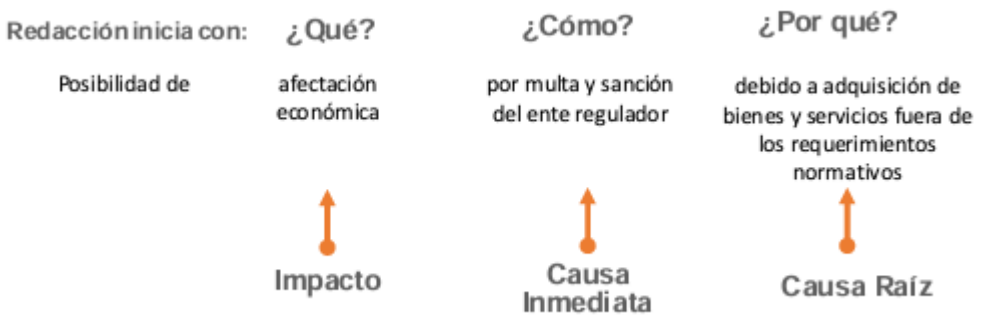
4.1 Identificación, descripción y clasificación de riesgos

Para iniciar la metodología, es importante consultar y analizar los aspectos relevantes del contexto estratégico, por parte de cada proceso.

A continuación, tomamos las estructuras propuestas por el DAFP para la redacción del riesgo y un ejemplo del mismo.



Ejemplo:



Asimismo, es necesario tener en cuenta las tipologías de riesgos definidas por el DAFP- 2022 y que se adoptarán en la Auditoría General de la República:

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 debida 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 un participante interno de la organización, cometido en 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: Fallas por negligencia o de naturaleza involuntaria, de las obligaciones frente a usuarios, que impiden satisfacer una obligación profesional frente a éstos.

Daños a activos fijos / eventos externos: Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos o eventos externos como atentados, vandalismo o perturbación del orden público.

Adicionalmente, se agregan las siguientes tipologías con análisis especial:

Riesgos de seguridad de la información y fiscales, según la guía del DAFP, los riesgos de soborno en cumplimiento de la norma técnica ISO37001 y los riesgos de lavado de activos y financiación del terrorismo, de acuerdo con la ley 2195 de 2022.

En este sentido tenemos las siguientes clasificaciones:

4.1.1 Riesgos de gestión u operativos.

En la fase de identificación de riesgos, se describe, se clasifica y se valora el riesgo. Se determina su probabilidad de ocurrencia y el impacto, obteniendo un nivel de riesgo inherente.

Los pasos siguientes los denominamos metodología general de riesgos.

Determinación de la probabilidad: se define de acuerdo con la Guía de la Función Pública, por tanto, se mide con la frecuencia en que se lleva a cabo la actividad generadora del riesgo así:

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por 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%

Aplica para riesgos de gestión, riesgos fiscales y riesgos de seguridad de la información.
Para dar claridad, tomamos el ejemplo del DAFP, de actividades y le frecuencia con que se llevan a cabo en la gestión:

Actividad	Frecuencia de la Actividad	Probabilidad frente al Riesgo
Planeación estratégica	1 vez al año	Muy baja
Actividades de talento humano, jurídica, administrativa	Mensual	Media
Contabilidad, cartera	Semanal	Alta
*Tecnología (incluye disponibilidad de aplicativos), tesorería *Nota: En materia de tecnología se tiene en cuenta 1 hora funcionamiento = 1 vez. Ej.: Aplicativo FURAG está disponible durante 2 meses las 24 horas, en consecuencia su frecuencia se calcularía 60 días * 24 horas= 1440 horas.	Diaria	Muy alta

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020

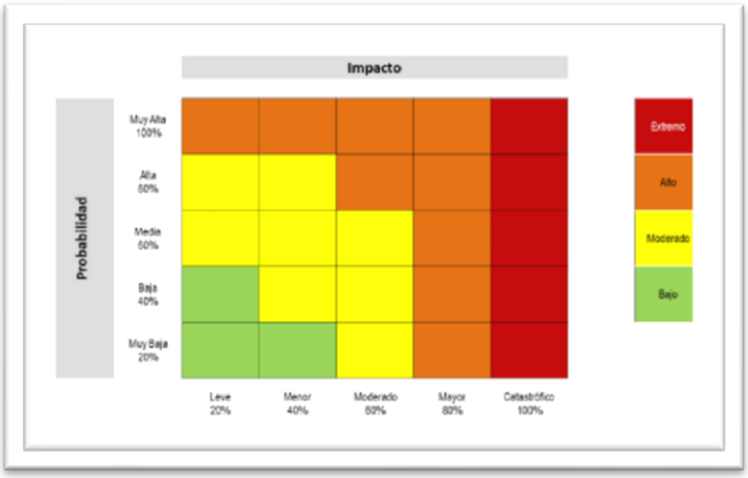
Determinación del impacto de los riesgos: Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales. Posteriormente se definen los criterios de los cinco (5) niveles, a saber: leve, menor, moderado, mayor y catastrófico

	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

Aplica para riesgos de gestión, riesgos fiscales y riesgos de seguridad de la información.

Como lo menciona la Guía de la Función Pública, “Frente al análisis de probabilidad e impacto no se utiliza criterio experto, esto quiere decir que el líder del proceso, como conocedor de su quehacer, define cuántas veces desarrolla la actividad, esto para el nivel de probabilidad, y es a través de la tabla establecida que se ubica en el nivel correspondiente, dicha situación se repite para el impacto, ya que no se trata de un análisis subjetivo.”

Como resultado se obtiene el nivel de riesgo inherente, que se muestra en un mapa de calor:



Aplica para riesgos de gestión, riesgos fiscales y riesgos de seguridad de la información.

4.1.2 Riesgos de seguridad de la información:

Identificación: Para esta etapa, se debe revisar los lineamientos de la política de seguridad de la información y su complementariedad con el modelo de seguridad y privacidad de la información (MSPI), del min tic, desarrollados en la Guía de la Función Pública.

Pasos a seguir:

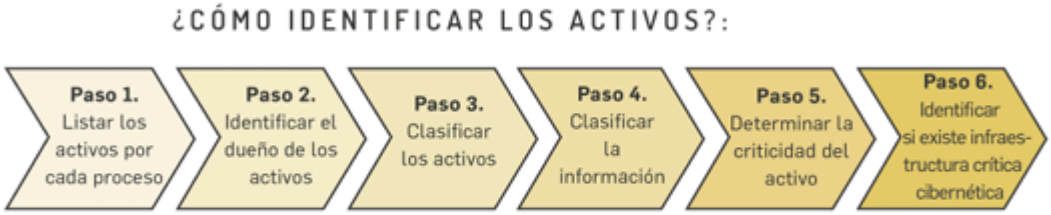
Identificación de los activos de seguridad de la información:

¿Qué son los activos?	¿Por qué identificar los activos?
Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como: -Aplicaciones de la organización	Permite determinar **qué es lo más importante que cada entidad y sus procesos poseen** (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios).

¿Qué son los activos?	¿Por qué identificar los activos?
-Servicios web -Redes -Información física o digital -Tecnologías de información TI -Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital	La entidad puede saber **qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano**, aumentando así su confianza en el uso del entorno digital.

Fuente: Actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública y Ministerio TIC, 2020

En este sentido se continua con la metodología de identificación de activos, según los siguientes pasos:



Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

Frente a la identificación de los riesgos de seguridad de la información, se definirán en la AGR los siguientes tres riesgos:

Pérdida de la confidencialidad
Pérdida de la integridad
Pérdida de la disponibilidad

Finalmente se continuará con las etapas de valoración del riesgo y definición de plan de acción, de acuerdo con la metodología general para la determinación de probabilidad e impacto y mapa de calor, donde se identifican los niveles de severidad de los riesgos.

4.1. 3 Riesgos fiscales:

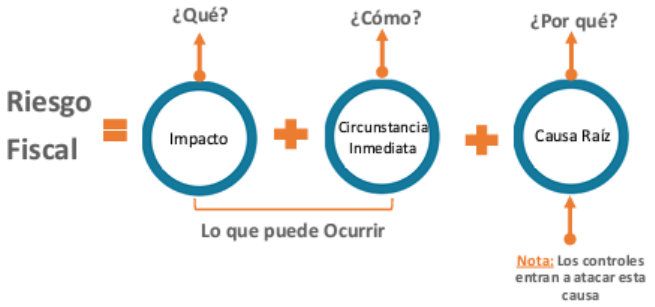
Teniendo en cuenta la estructura y elementos de la definición de riesgos que tiene la guía de la Función Pública, la cual es armónica con la norma ISO 31000, define riesgo fiscal, así:

> ***Efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.***

Para la identificación del riesgo fiscal es necesario establecer los puntos de riesgo fiscal y las circunstancias Inmediatas.

Los puntos de riesgos son situaciones en las que potencialmente se genera riesgo fiscal, es decir, son aquellas actividades de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos, así como a la recaudación, manejo e inversión de sus rentas- (Artículo 3 Ley 610 de 2000).
Identificación de áreas de impacto: Dentro del contexto de riesgo fiscal, el área de impacto siempre corresponderá a una consecuencia económica sobre el patrimonio público, a la cual se vería expuesta la organización en caso de materializarse el riesgo.

Identificación de la causa raíz o potencial hecho generador La causa raíz sería cualquier evento potencial (acción u omisión) que de presentarse provocaría un menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro (Auditoría General de la República, 2015).



Ejemplo:

¿Qué?	¿Cómo?	¿Por qué?
Posibilidad de efectos dañoso sobre **bienes públicos**	por pérdida, extravío o hurto de bienes muebles de la entidad.	a causa de la omisión en la aplicación del procedimiento para el ingreso y salida de bienes del almacén

4.1.4 Riesgos de corrupción:

En esta tipología tenemos la identificación de riesgos de soborno, los cuales se gestionarán de acuerdo con la metodología de la NT ISO 37001.

De acuerdo con la Ley 2195 de 2022, se identificarán los riesgos de lavado de activos y financiación del terrorismo (LAFT), en cumplimiento de la Ley 2195 de 2022.

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.

En cuanto a probabilidad e impacto de los riesgos de corrupción, se manejarán criterios diferente de acuerdo con la metodología.

A continuación, se presentan los criterios para determinar probabilidad:

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.

Para determinar el impacto de los riesgos de corrupción, se presentan los siguientes criterios:

N.°	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...	RESPUESTA	
		SÍ	NO
1	¿Afectar al grupo de funcionarios del proceso?	X	
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?	X	
3	¿Afectar el cumplimiento de misión de la entidad?	X	
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		X
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?	X	
6	¿Generar pérdida de recursos económicos?	X	
7	¿Afectar la generación de los productos o la prestación de servicios?	X	
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		X
9	¿Generar pérdida de información de la entidad?		X
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?	X	
11	¿Dar lugar a procesos sancionatorios?	X	
12	¿Dar lugar a procesos disciplinarios?	X	
13	¿Dar lugar a procesos fiscales?	X	
14	¿Dar lugar a procesos penales?		X
15	¿Generar pérdida de credibilidad del sector?		X
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		X
17	¿Afectar la imagen regional?		X
18	¿Afectar la imagen nacional?		X
19	¿Generar daño ambiental?		X
Responder afirmativamente de UNA a CINCO pregunta(s) genera un impacto moderado. Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor. Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico.		**10**	
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad.		

Nivel de impacto MAYOR

4.2 Valoración de riesgos

Para la valoración, se cuenta inicialmente con el análisis previo de riesgos: en este punto se ha establecido la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto.

Evaluación de riesgos: a partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE).

De acuerdo con el resultado, los líderes de procesos deben identificar los controles existentes o formular nuevos controles, si no existieran, con el fin de reducir la probabilidad o el impacto.

Valoración de controles: en primer lugar, conceptualmente un control se define como la medida que permite reducir o mitigar el riesgo. Para la valoración de controles se debe tener en cuenta:

- ✓ La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso sí aplica el criterio experto.
- ✓ Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

Estructura para la definición de controles:

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.

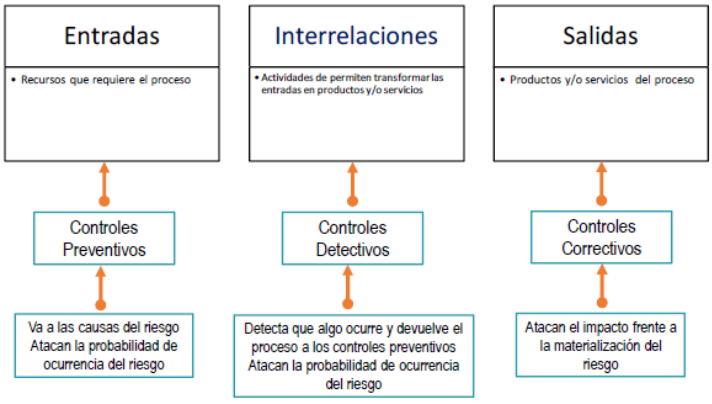
Complemento: corresponde a los detalles que permiten identificar claramente el objeto del control.

Tipología de controles:

Control preventivo: control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.

Control detectivo: control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.

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



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

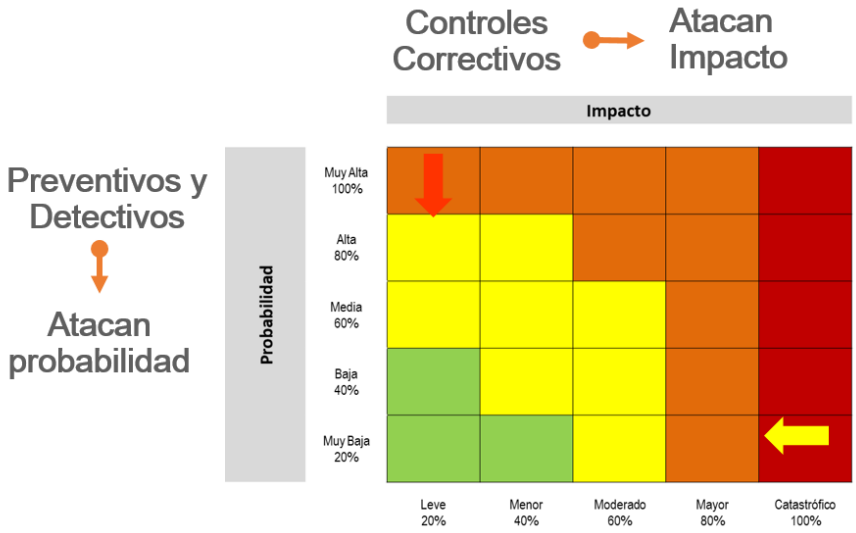
Así mismo, de acuerdo con la forma como se ejecutan tenemos:

Control manual: controles que son ejecutados por personas.

Control automático: son ejecutados por un sistema.

Según el resultado de los controles aplicados se obtiene el RIESGO RESIDUAL, identificado con el mismo mapa de calor presentado anteriormente.

Movimiento en la matriz de calor acorde con el tipo de control



4.3 Estrategias para combatir riesgos:

Por último y de acuerdo con la zona de riesgo, se define el "**Plan de Acción"**, en el que se determinan las acciones a desarrollar para los riesgos, de acuerdo con su tipología y los niveles de aceptación. Todas estas actividades se realizan a través del sistema de información SIA POAS, que facilita los cálculos de probabilidad e impacto, a través de las opciones de selección desplegables, que nos dan un resultado numérico.

Con el resultado del RIESGO RESIDUAL, se definen las siguientes acciones:

ACEPTAR. Se determina para los riesgos cuyo resultado, una vez aplicados los controles, se encuentra en el nivel de RIESGO RESIDUAL LEVE o MENOR. Estos riesgos requieren monitoreo y seguimiento periódico por parte de los líderes de procesos. En esta opción se considera la opción **TRANSFERIR**, cuando se considera que la mejor estrategia es tercerizar o trasladar el riesgo a través de pólizas.

EVITAR. Decisión que se adopta cuando después de un análisis se considera que el riesgo es demasiado alto y lo mejor es NO asumir la actividad que genera el riesgo y por tanto plantear una

diferente.

REDUCIR. Se determina para los riesgos cuyo resultado, una vez aplicados los controles, se encuentran en el nivel MODERADO, ALTO o CASTASTROFICO. Estos riesgos requieren monitoreo y seguimientopermanente por parte de los líderes de procesos y, además, exigen la formulación de plan de acción.

Para los riesgos de corrupción, incluidos los riesgos de soborno y lavado de activos y financiación del terrorismo, no hay aceptación. En consecuencia, este tipo de riesgos no podrán valorarse en un nivel residual leve o menor, por tanto, siempre requerirán la definición de acciones para reducir el nivel del riesgo.

Este plan deberá formularse a través del SIA POAS, en el módulo administración de riesgos, y recogerá entre otras, la siguiente información:

Riesgo	Plan de Acción	Responsable	Fecha Inicio	Fecha Fin	Indicador de cumplimiento de la Acción	Fecha de Seguimiento.	Observación de la Oficina de Control Interno

5. SEGUIMIENTO Y EVALUACIÓN DEL MAPA DE RIESGOS

- Monitoreo: en concordancia con la cultura del autocontrol al interior de la entidad, los líderes de los procesos junto con su equipo realizarán monitoreo y evaluación permanente a la gestión de riesgos.

- Seguimiento: el jefe de control interno o quien haga sus veces debe adelantar seguimiento a la gestión de riesgos. En este sentido es necesario que en sus procesos de auditoría interna analice las causas, los riesgos y la efectividad de los controles incorporados en el mapa de riesgos institucional.

Los líderes de proceso monitorean constantemente los controles definidos para los riesgos y las acciones del plan de acción, cuando haya lugar. Además, registran con periodicidad trimestral en el SIA POAS el seguimiento de los mismos.

La Oficina de Planeación, cumplirá con las acciones de monitoreo de acuerdo con las responsabilidades como segunda línea de defensa, y de acuerdo con el procedimiento interno de la AGR, de manera trimestral.

La Oficina de Control Interno lleva a cabo el seguimiento a la administración del riesgo, de conformidad con lo indicado en los documentos “Guía rol de las unidades u oficinas de control interno, auditoría interna o quien haga sus veces” y como se determina en el título precedente de Roles y Responsabilidades.

La Oficina de Control Interno presentará un informe trimestral sobre los resultados de la evaluación de la efectividad del Sistema de Control Interno - SCI, acorde con la evaluación de los controles definidos en los mapas de riesgos y de los riesgos de procesos, en el cual se consigne, cuando sea el caso, la materialización, la creación, la modificación o la eliminación de alguno de los riesgos.

- Primer seguimiento: con corte al 30 de marzo. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días del mes de abril.
- Segundo seguimiento: con corte al 30 de junio. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de Julio.
- Tercer seguimiento: con corte al 30 de septiembre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de octubre.
- Cuarto seguimiento: con corte al 30 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de enero.

El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en la página web de la entidad o en un lugar de fácil acceso para el ciudadano.

En especial deberá adelantar las siguientes actividades:

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

Acciones a seguir en caso de materialización de riesgos de corrupción
En el evento de materializarse un riesgo de corrupción, es necesario realizar los ajustes necesarios con acciones, tales como:

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

La Oficina de Control Interno debe asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma oportuna y efectiva.

Las acciones adelantadas se refieren a:

■ Determinar la efectividad de los controles.
■ Mejorar la valoración de los riesgos.
■ Mejorar los controles.

■ Analizar el diseño e idoneidad de los controles y si son adecuados para prevenir o mitigar los riesgos de corrupción.
■ Determinar si se adelantaron acciones de monitoreo.
■ Revisar las acciones del monitoreo.

GLOSARIO

Activo de información: 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.
Amenaza: situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
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 raíz: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo
CIGD: Comité Institucional de Gestión y Desempeño.
CICCI: Comité Institucional de Coordinación de Control Interno
Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.
Consecuencia: los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
Contingencia: posible evento futuro, condición o eventualidad.
Control: Medida que permite reducir o mitigar un riesgo
Crisis: ocurrencia o evento repentino, urgente, generalmente inesperado que requiere acción inmediata.
Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.
Debida diligencia: proceso para evaluar con mayor detalle la naturaleza y alcance del riesgo de soborno y para ayudar a las organizaciones a tomar decisiones en relación con transacciones, proyectos, actividades, socios de negocios y personal específicos (ISO 37001:2016)
Factores de riesgo: Son las fuentes generadoras de riesgos.
Incertidumbre: Incertidumbre es el estado, incluso parcial, de deficiencia de información relacionada con la comprensión o conocimiento de un evento, su consecuencia o su posibilidad. (ISO 37001:2016)
Impacto: las consecuencias que puede ocasionar a la organización la materialización del riesgo.
Integridad: Propiedad de exactitud y completitud.
Mapa de Riesgos: documento que resume los resultados de las actividades de gestión de riesgos,incluye una representación gráfica en modo de mapa de calor de los resultados de la evaluación deriesgos.

MIPG: Modelo Integrado de Planeación y Gestión.
Nivel de riesgo: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia deun evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.
Probabilidad: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición alriesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número deveces que se pasa por el punto de riesgo en el periodo de un año.

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales, como 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 corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta pueda explotaruna vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarsecomo una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27001).
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.
SIA POAS: Sistema Integral de Auditoría, aplicativo propio para la gestión de la planeación estratégica, los riesgos, los planes de mejora y los indicadores.
Soborno: Oferta, promesa, entrega, aceptación o solicitud de una ventaja indebida de cualquier valor (que puede ser de naturaleza financiera o no financiera), directamente o indirectamente, e independiente de su ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o deje de actuar en relación con el desempeño de las obligaciones de esa persona
Nota 1 Lo anterior es una definición genérica. El significado del término “soborno” es el definido por las leyes antisoborno aplicables a la organización y por el sistema de gestión antisoborno diseñado por la organización. (ISO 37001:2016)
Socio de negocios: parte externa con la que la organización, tiene, o planifica establecer, algún tipo de relación comercial. (ISO 37001:2016)

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

REFERENCIAS

Departamento Administrativo de la Función Pública- DAFP. Guía para la Administración del Riesgo y diseño de controles en entidades públicas. Versión 6. 2022