POLÍTICA DE ADMINISTRACIÓN DE RIESGOS EN EL INSTITUTO DISTRITAL DE RECREACIÓN Y DEPORTE IDRD

Versión 6

BOGOTÁ D.C

2023

ÍNDICE

1. OBJETIVO

Presentar los lineamientos y etapas para gestionar los riesgos de la entidad.

2. ALCANCE

Aplica a los riesgos de gestión, seguridad de la información, corrupción, lavado de activos y financiación del terrorismo identificados en los procesos de la entidad.

Para los riesgos ambientales y de seguridad y salud en el trabajo se indican únicamente responsabilidades generales para los coordinadores de estos sistemas en su rol de segunda línea de defensa.

Para los riesgos en los procesos de contratación se menciona bajo que metodología se realiza el monitoreo.

3. DEFINICIONES

Apetito de riesgo: Es el nivel de riesgo que la entidad puede aceptar.

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 para que se presente el riesgo.

Causa Raíz: Causa principal, corresponde a las razones por las cuales se puede presentar el riesgo.

Consecuencia: Los efectos o situaciones resultantes de la materialización del riesgo

Control: Medida que permite reducir o mitigar un riesgo.

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

Nivel de riesgo: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.

Materialización: Evento que provocó la ocurrencia del riesgo

Probabilidad: Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

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.

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

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

Contraparte: es cualquier persona natural o jurídica con la que el Distrito Capital tiene o planifica establecer algún tipo de relación comercial. En esta categoría se ubican contrapartes como proveedores de bienes y servicios, empleados en cualquier modalidad de contratación y clientes.

Debida diligencia: es el proceso mediante el cual la entidad adopta medidas para el conocimiento de la contraparte, de su negocio, operaciones, y productos y el volumen de sus transacciones (Superintendencia de Sociedades de Colombia, 2021).

Financiación del terrorismo - FT: la financiación del terrorismo está relacionada con los fondos, bienes o recursos a los que acceden las organizaciones terroristas o los terroristas para poder costear sus actividades (UIAF, 2013).

Lavado de activos – LA: el lavado de activos es un delito que consiste en dar una apariencia lícita o de legalidad a bienes, dinerarios o no, que en realidad son productos o "ganancias" de delitos como tráfico ilícito de drogas, trata de personas, corrupción, secuestros y otros (UNODC, 2021).

Listas vinculantes: son aquellas listas de personas y entidades asociadas con organizaciones terroristas que son vinculantes para Colombia bajo la legislación y conforme al derecho internacional, de acuerdo con el artículo 20 de la Ley 1121 de 200616. Entre estas listas se encuentran las resoluciones del Consejo de seguridad de las Naciones Unidas.

Listas restrictivas: son aquellas listas frente a las cuales la empresa se abstendrá o buscará terminar relaciones jurídicas o de cualquier otro tipo con las personas naturales o jurídicas que en ellas figuren. Tienen esta característica las listas de las Naciones Unidas, las listas OFAC y las otras listas que por su naturaleza generen un alto riesgo que no pueda mitigarse con la adopción de controles. (UNODC, 2021)

Operación inusual: es aquella operación cuya cuantía o características no guardan relación con la actividad económica ordinaria o normal del asociado/cliente o que, por su número, cantidad, periodicidad o características no se ajusta a las pautas de normalidad establecidas por la organización para un sector, una industria o una clase de contraparte, o no tiene un fundamento (Superintendencia de la Economía Solidaria, 2016).

Oficial de cumplimiento o equipo encargado: es la persona natural designada por la entidad vigilada, encargada de promover, desarrollar y velar por el cumplimiento de los procedimientos específicos de prevención, actualización y mitigación del riesgo LA/FT (Superintendencia de Sociedades de Colombia, 2021). Las entidades no vigiladas no tienen un oficial de cumplimiento, y, en principio, deben establecer un equipo de trabajo que asuma sus funciones.

Operación sospechosa: cualquier acción o información relevante sobre manejo de activos, pasivos u otros recursos, cuya cuantía o características que no guarden relación con la actividad económica de sus asociados, o sobre las transacciones de asociados/clientes o usuarios que, por su número, por las cantidades transadas o por las características particulares de las mismas, puedan conducir razonablemente a sospechar que los mismos están usando a la organización para transferir, manejar, aprovechar o invertir dineros o recursos provenientes de actividades delictivas o destinados a su financiación (Superintendencia de la Economía Solidaria, 2016).

4. MARCOS DE REFERENCIA

Para los riesgos de gestión, seguridad de la información y corrupción se utiliza como marco de referencia la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas versión 5, emitida por el Departamento Administrativo de la Función Pública.

Para los riesgos de lavado de activos y financiación del terrorismo – LAFT se utiliza como marco de referencia el documento técnico Adaptación de medidas de prevención y mitigación del riesgo del lavado de activos, financiación del terrorismo en las entidades del Distrito Capital, emitido por la Secretaría Mayor de la Alcaldía de Bogotá en diciembre de 2022.

Para los riesgos de los procesos contractuales se utiliza como marco de referencia el Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación expedido por Colombia Compra Eficiente.

5. RIESGOS INSTITUCIONALES

Se establece el mapa de riesgos institucional con el fin de que la alta dirección cuente con un panorama de los riesgos más representativos en la entidad de acuerdo con los siguientes criterios de selección:

Criterios selección mapa riesgos institucional

Tipo	Criterios de selección
Riesgos de gestión	-Riesgos asociados al cumplimiento de la misión - Riesgos en zona residual alta o extrema.
Riesgos de corrupción- LAFT	Todos los riesgos identificados.
Riesgos de seguridad de la información	Riesgos asociados al tipo de activo de información con su respectiva amenaza y vulnerabilidad.
Riesgos de seguridad y salud en el trabajo	Riesgos cuya interpretación del nivel de probabilidad se encuentre en muy alto.
Riesgos ambientales	Riesgos en zona residual alta o muy alta.
Riesgos en los procesos de contratación	Riesgos en zona residual media, alta o extrema.

6. ROLES Y RESPONSABILIDADES

La administración del riesgo (de gestión, seguridad de la información, corrupción y LAFT) se desarrolla bajo el esquema de las líneas de defensa, modelo de control que establece y clasifica los roles y responsabilidades de todos los actores del riesgo, para proporcionar aseguramiento de la gestión y prevenir la materialización de los riesgos. Los roles establecidos son:

- Línea estratégica
- Primera línea de defensa
- Segunda línea de defensa
- Tercera línea de defensa

En las siguientes tablas se describen las responsabilidades por cada uno de estos roles:

Responsabilidades frente a la gestión del riesgo para la línea estratégica

LÍNEA ESTRATÉGICA		
RESPONSABLES		
Alta Dirección (Nota: Los integrantes de la Alta Dirección son los quehacen parte del Comité Institucional Gestión y Desempeño los cuales se mencionan en el artículo 3°de la Resolución 265 de 2020)		**Comité Institucional de Coordinación de Control Interno (CICCI)**
Responsabilidades frente al riesgo	▪ Revisar y ajustar (cuando sea pertinente) la política de administración del riesgo de la entidad de acuerdo con los lineamientos emitidos por los entes competentes en el tema o las dinámicas de mejora continua que se presenten en la gestión de riesgos del Instituto	▪ Someter a aprobación del representante legal la política de administración de riesgos.
	▪ Evaluar la aplicación de la política de administración del riesgo a través del informe suministrado por la Oficina Asesora de Planeación (segunda línea de defensa), así como de la información presentada por la tercera línea de defensa al Comité Institucional de Coordinación de Control Interno con énfasis en los riesgos que se han materializado con el fin de que los procesos tomen medidas oportunas y eficaces para evitar la posible repetición de los mismos.	▪ Hacer seguimiento a la implementación de la gestión del riesgo, de acuerdo con la información clave reportada por la segunda línea de defensa y a los resultados de las evaluaciones realizadas por Control Interno, las cuales incluyen los riesgos materializados con el fin de que se tomen las medidas oportunas y eficaces para evitar repeticiónde los mismos

Responsabilidades frente a la gestión del riesgo para la primera línea de defensa

P R I M E R A L I N E A	
Responsables	
Responsables de los procesos	
	▪ Identificar y actualizar los riesgos de gestión y corrupción teniendo en cuenta los factores que los originan, los cuales se encuentran descritos en el numeral 9.1 de este documento ▪ Diseñar y valorar los controles para reducir o mitigar los riesgos de gestión y de corrupción, así como los de LAFT en los procesos que aplique. ▪ Implementar los controles establecidos para reducir o mitigar los riesgos de gestión y

Responsabilidades frente al riesgo	de corrupción, así como los de LAFT en los procesos que aplique. ▪ Documentar en los procedimientos los controles para abordar los riesgos de gestión. ▪ Tratar los riesgos residuales de gestión, corrupción y LAFT, cuando apliquen, mediante la definición de planes e implementación oportuna de los mismos con el fin de reducir las probabilidades de materialización. ▪ Reportar en los plazos establecidos por la segunda línea de defensa (OAP) el monitoreo a los riesgos. ▪ Realizar las mediciones de los indicadores y analizar los resultados tomando las acciones en caso de incumplimientos. ▪ En el caso que se materialice un riesgo, reportarlo en el instrumento de monitoreo de riesgos con el fin de analizar la situación con el equipo de trabajo de la Oficina Asesora de Planeación para determinar las acciones a implementar. ▪ Analizar los informes emitidos por la segunda y tercera línea de defensa con el fin de proponer mejoras para la gestión del riesgo. ▪ En caso de presentarse la materialización de un riesgo no identificado en el mapa, debe solicitar el acompañamiento a la Oficina Asesora de Planeación para actualizar el mismo.
Gerentes de proyecto	
	▪ Monitorear los riesgos descritos en las fichas de la Metodología General Ajustada MGA, que sean competencia directa de la gerencia del proyecto asociados al riesgo "*Baja ejecución de metas de los proyectos de inversión".* En este monitoreo deben participar los responsables de los procesos que inciden en la gestión del proyecto de inversión y puedan afectar una eventual materialización del riesgo.

Responsabilidades frente a la gestión del riesgo para la segunda línea de defensa

S E G U N D A L I N E A		
Responsables		
Oficina Asesora de Planeación		**Responsable del Sistema de Gestión de Seguridad y Salud en elTrabajo** **Responsable del SistemaAmbiental**
	▪ Orientar a la línea estratégica en la definición y actualización de la política de administración de riesgos en el IDRD. ▪ Coordinar con los procesos la actualización de	▪ Gestionar los riesgos ambientales conforme a lo definido en la normatividad ambiental aplicable al Plan Institucional de Gestión Ambiental – PIGA, en lo relacionado con la identificación y evaluación de aspectos e impactos ambientales.

Responsabilidades frente al riesgo	los riesgos de gestión, corrupción y LAFT, teniendo en cuenta los factores que los originan los cuales seencuentran descritos en el numeral 9.1 de este documento. ▪ Revisar junto con la primera línea de defensa el diseño de los controles, los planes para su tratamiento y la definición de indicadores. ▪ Elaborar informe cuatrimestral, utilizando como insumo la información reportada por la primera línea de defensa en el instrumento de monitoreo de riesgos. ▪ Administrar base histórica de eventos que corresponden a los riesgos materializados	▪ Gestionar los riesgos de seguridad y salud en el trabajo, de acuerdo con la metodología definida en la Guía Técnica Colombiana para la Identificación de los Peligros y la Valoración de los Riesgos en Seguridad y Salud Ocupacional GTC - 45 o aquella que la modifique o sustituya.
		▪ Identificar los peligros y riesgos de seguridad y salud en el trabajo a los cuales están expuestos los funcionarios y contratistas de la entidad, así como los controles operacionales para mitigar su impacto.
		▪ Socializar, implementar y hacer seguimiento a los controles operacionales asociados a los riesgos de seguridad y salud en el trabajo, así como los ambientales
		▪ Actualizar las matrices de los riesgos definidos en seguridad y salud en el trabajo, así como las ambientales
		▪ Determinar los riesgos ambientales en la entidad, así como los controles operacionales necesarios para mitigar la probabilidad de ocurrencia y/o evitar su materialización.
		▪ Monitorear los riesgos ambientales y de seguridad y salud en el trabajo
		▪ Presentar a la Alta Dirección informe de monitoreo semestral a la gestión de riesgos.

Responsabilidades frente a la gestión del riesgo para la tercera línea de defensa

T E R C E R A L I N E A	
Responsables	
Oficina de Control Interno	
Responsabilidades frente al riesgo	▪ Proponer al Comité Institucional de Coordinación de Control Interno el plan anual de auditoría basado en riesgos, priorizando aquellos procesos y/o asuntos de mayor exposición según los criterios definidos por el DAFP en su Guía de Auditoría para Entidades Públicas. ▪ Hacer seguimiento y evaluación objetiva e independiente de la gestión del riesgo de la entidad, informar los hallazgos y proporcionar recomendaciones. ▪ Brindar asesoría, orientación técnica y recomendaciones frente a la administración del riesgo ▪ Monitorear la exposición de la entidad al riesgo y realizar recomendaciones con alcance preventivo. ▪ Asesorar de forma proactiva y estratégica a la Alta Dirección y los líderes de proceso, en materia de control interno y sobre la administración del riesgo. ▪ Sensibilizar a la alta dirección y a todos los niveles de la entidad sobre las responsabilidades en materia de riesgos.

7. APETITO DEL RIESGO

El apetito del riesgo de la entidad es el que se ubica en el nivel “bajo”, luego de aplicar los controles y por consiguiente no requiere generar acciones adicionales, lo que no significa que no deban monitorearse para asegurar que permanezcan en este nivel y se tomen las medidas necesarias en el evento en que el mismo se modifique.

Es importante señalar que los riesgos de corrupción y LAFT no se pueden ubicar en nivel “bajo”por su naturaleza.

8. TOLERANCIA AL RIESGO

Es la variación permitida del resultado de los indicadores definidos para los riesgos frente a la meta establecida para evaluar la necesidad de tomar o no acciones correctivas. La entidad establece que el no cumplimiento de una meta requiere la toma de estas acciones. Es decir, la tolerancia al riesgo (gestión, corrupción, seguridad de la información y LAFT) es cero (0%).

9. ETAPAS PARA LA GESTIÓN DE RIESGOS

9.1. IDENTIFICACIÓN DEL RIESGO:

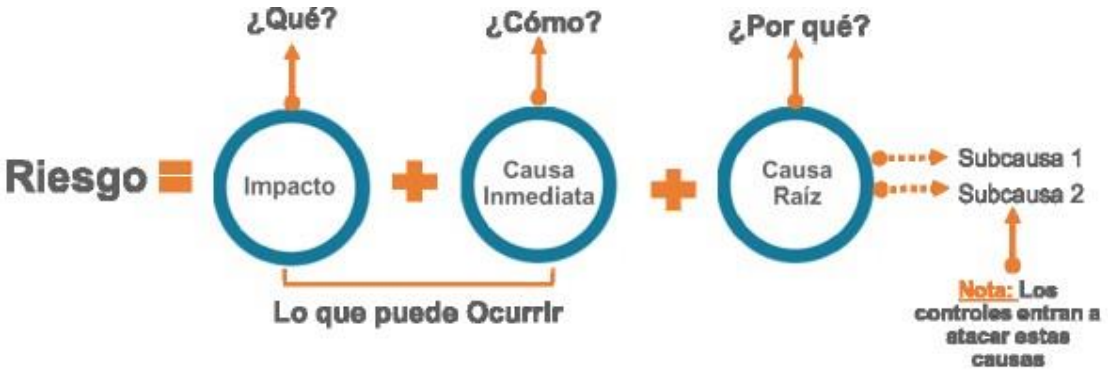
Los riesgos se pueden identificar por medio de las siguientes fuentes, entre otras:

- Análisis del contexto externo e interno realizado en cada cambio de administración distrital o cuando surgen situaciones emergentes. En este caso la actualización se realiza durante los tres meses siguientes a la armonización presupuestal que se gestiona para la puesta en marcha de un nuevo Plan Distrital de Desarrollo.
- Eventos adversos que puedan presentarse e inciden en el cumplimiento delos objetivos estratégicos y del proceso.
- Actividades establecidas en el flujo de los procedimientos que inciden en el cumplimiento del objetivo del proceso.
- Análisis de las PQRS cuya repetición o impacto afectan la satisfacción de los usuarios.
- Implementación inadecuada de requisitos legales ante posibles cambios normativos.
- Evaluaciones realizadas por entes externos de control cuyo resultado impacta la gestión institucional.
- Observaciones y recomendaciones procedentes de las auditorias de control interno.
- Modificaciones en activos de información

NOTAS:

1. El IDRD actualiza las matrices de riesgos con una frecuencia anual y se hará en el primer –semestre de la vigencia. En caso de cambio de administración, la actualización se realiza durante los tres meses siguientes a la armonización presupuestal que se gestiona para la puesta en marcha de un nuevo Plan Distrital de Desarrollo.
2. La primera línea de defensa nunca debe detener la implementación de los controles que se presentan en las matrices de riesgos.
3. En el mapa de riesgos se lleva la trazabilidad de las revisiones y cambios según corresponda.

Los riesgos se describen a través de la siguiente estructura:



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

Donde:

Impacto: Corresponde a las consecuencias que puede ocasionar a la entidad la materialización del riesgo. El área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta el proceso o entidad en caso de materializarse el riesgo.

Causa inmediata: Define las circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo

Causa raíz: Es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir
más de una causa o subcausas que pueden ser analizadas.

Ejemplo:

Redacción inicia con:	¿Qué?	¿Cómo?	¿Por qué?
Posibilidad de	IMPACTO afectación económica	CAUSA INMEDIATA por multa y sanción del ente regulador	CAUSA RAÍZ debido a la adquisición de bienes y servicios fuera de los requerimientos normativos

Para los riesgos de corrupción es necesario que en su redacción concurran los componentes de su definición, así: Acción u omisión + Uso del poder + Desviación de la gestión de lo público + El beneficio privado.

9.2 CLASIFICACIÓN DEL RIESGO. 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	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y 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/eventos externos como atentados, vandalismo, orden público.

9.3 ANÁLISIS DEL RIESGO

RIESGOS DE GESTIÓN, SEGURIDAD DE LA INFORMACIÓN

En esta etapa se determina la probabilidad de ocurrencia del riesgo la cual está asociada al número de veces en que la actividad que conlleva al riesgo se realiza en periodos anuales. A continuación se presentan los criterios para definir el nivel de probabilidad

Criterios para definir el nivel de probabilidad

Nivel de probabilidad	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%

El impacto determina la forma en la que la entidad mide el efecto o la consecuencia de la materialización del riesgo. Para calificarlo se tiene en cuenta el impacto económico y reputacional conforme a los criterios:

Criterios para definir el nivel de impacto

	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

NOTA:
Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto, así, por ejemplo: para un riesgo identificado se define un impacto económico en nivel insignificante e impacto reputacional en nivel moderado, se tomará el más alto, en este caso sería el nivel moderado.

RIESGOS DE CORRUPCIÓN Y LAFT

Los criterios para definir el nivel de **probabilidad:**

Nivel de probabilidad para riesgos de corrupción.

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.

Los criterios para calcular el **nivel de impacto:**

Criterios para calificar el impacto – riesgos de corrupción

No.	Pregunta: Si el riesgo de corrupción se materializa podría…	Respuesta	
		Si	No
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de misión de la entidad?		
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		
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?		

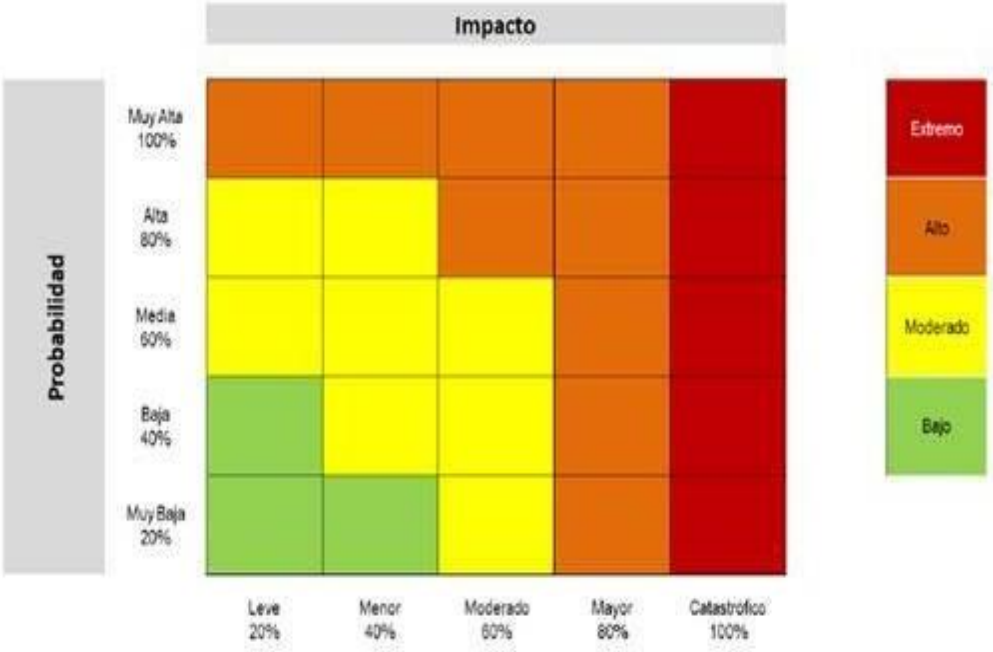
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		
9	¿Generar pérdida de información de la entidad?		
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?		
11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar 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?		

No.	Pregunta: Si el riesgo de corrupción se materializa podría…	Respuesta	
		Si	No
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		
Si se responde afirmativamente de 1 a 5 preguntas, el impacto es **Moderado** (genera medianas consecuencias para la entidad). Si se responde afirmativamente de 6 a 11 preguntas, el impacto es **Mayor** (genera altas consecuencias para la entidad). Si se responde afirmativamente de 12 a 19 preguntas, el impacto es **Catastrófico** (genera consecuencias desastrosas para la entidad).			

Para los riesgos de corrupción y LAFT, el análisis de impacto se realiza teniendo en cuentasolamente los niveles “moderado”, “mayor” y “catastrófico”, dado que estos riesgos siempre serán significativos; en este orden de ideas, no aplican los niveles de impacto insignificante y menor, que sí aplican para los demás riesgos.

Una vez se obtenga el impacto y la probabilidad para cada riesgo se ubica en las calificaciones respectivas en la fila y columna correspondiente sobre el mapa de calor obteniendo así el nivel de riesgo inherente, es decir, antes de controles. Ver figura:

Mapa de calor (matriz de calificación)



9.4 EVALUACIÓN DEL RIESGO DE GESTIÓN, CORRUPCIÓN, LAFT Y SEGURIDAD DE LA INFORMACIÓN

La evaluación comprende el diseño y la valoración de los controles. Sus variables son:

Variables para el diseño de controles

Variable	Descripción
Responsable de ejecutar el control	Persona asignada para ejecutar el control. Debe tener la autoridad, competencias y conocimientos para ejecutar el control dentro del proceso. Cuando el control se hace de manera manual (ejecutado por personas) es necesario establecer el cargo responsable de su realización. Si lo hace un sistema o aplicación de manera automática, a través de una plataforma tecnológica, es importante establecer como responsable de ejecutar el control al sistema o aplicación respectivo.
Propósito (acción)	El control debe tener un propósito que indique para qué se realiza, y que ese propósito conlleve a prevenir, detectar o corregir las causas que generan el riesgo. Los verbos que se deben utilizar son: • Verificar • Validar • Conciliar • Comparar • Revisar • Cotejar No se deben utilizar verbos como: • Elaborar • Diseñar • Programar • Solicitar • Divulgar
Cómo se realiza la actividad de control (complemento)	El control debe indicar detalladamente el cómo se realiza
Periodicidad	El control debe tener una periodicidad específica para su realización (diario, mensual, trimestral, anual, etc.) y su ejecución debe ser consistente y oportuna para la mitigación del riesgo. Pueden existir controles que no tienen una periodicidad específica, en cuyo caso su redacción debe quedar de tal forma que indique que cada vez que se desarrolla la actividad se ejecuta el control.
Qué pasa con las observaciones o desviaciones	Describir detalladamente las acciones a seguir cuando se presentan desviaciones u observaciones como resultado de ejecutar el control.

Evidencia de la ejecución del control	El control debe dejar evidencia de su ejecución. Esta evidencia ayuda a que se pueda revisar la misma información por parte de un tercero y llegue a la misma conclusión de quien ejecutó el control, y se pueda evaluar que el control realmente fue ejecutado de acuerdo con las variables descritas anteriormente.

Los controles contrarrestan las causas del riesgo y se clasifican en:

Preventivos. Evita que ocurra el riesgo y deben ser aplicados antes de que se realice la actividad que origina el riesgo.

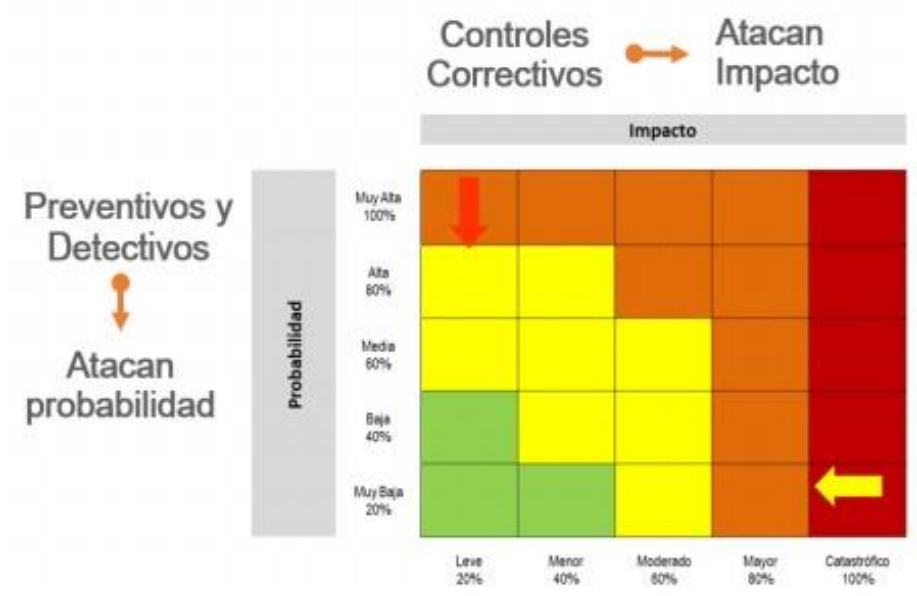
Detectivos. Detectan el riesgo durante la ejecución de la actividad que lo origina

Correctivos. Actúan posterior a la materialización el riesgo y deben estar identificados para todos los riesgos de gestión, seguridad la información, corrupción y LAFT.

NOTA. Para los riesgos de corrupción este tipo de control corresponde al plan de contingencia

Los controles preventivos y detectivos reducen la probabilidad y los correctivos, el impacto en el sentido que presenta la figura:

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



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

La evaluación de los controles se realizade acuerdo con:

Evaluación de controles- Gestión y Seguridad de la Información

Características			Descripción	Peso
Atributos de eficacia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
*Atributos informativos	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	N.A
		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.	N.A
	Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.	N.A
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	N.A
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.	N.A
		Sin registro	El control no deja registro de la ejecución del control.	N.A

Evaluación de controles- Corrupción y LAFT

CRITERIO DE EVALUACIÓN	OPCIÓN DE RESPUESTA AL CRITERIO DE EVALUACIÓN	PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL
Asignación del responsable	Asignado	15
	No asignado	0
Segregación y autoridad del responsable	Adecuado	15
	Inadecuado	0
Periodicidad	Oportuna	15
	Inoportuna	0
Propósito	Prevenir	15
	Detectar	10
	No es un control	0
Cómo se realiza la actividad de control	Confiable	15
	No confiable	0
Qué pasa con las observaciones o desviaciones	Se investigan y resuelven oportunamente	15
	No se investigan y resuelven oportunamente	0
Evidencia de la ejecución del control	Completa	10
	Incompleta	5
	No existe	0

9.5 DETERMINACIÓN DEL NIVEL DE RIESGO RESIDUAL PARA GESTIÓN, CORRUPCIÓN, SEGURIDAD DE LA INFORMACIÓN Y LAFT

Con el resultado de valoración de la probabilidad y del impacto, así como de la evaluación de los controles, se determina el riesgo residual. A continuación, se presenta un ejemplo:

Proceso: Adquisición de bienes y servicios

Objetivo: Adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación.

Riesgo: Posibilidad de afectación económica por multa y sanción del ente regulador debido a la adquisición de bienes y los servicios sin el cumplimiento de los requisitos normativos.

Probabilidad Inherente: Moderada 60%

Impacto Inherente: Mayor 80%

Zona de riesgo: Alta

Controles identificados:

Control 1: El profesional del área de contratos verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor, los contratos que cumplen son registrados en el sistema de información de contratación.

Control 2: El jefe del área de contratos verifica en el sistema de información de contratación la información registrada por el profesional asignado y aprueba el proceso para firma del ordenador del gasto, en el sistema de información queda el registro correspondiente, en caso de encontrar inconsistencias, devuelve el proceso al profesional de contratos asignado.

Aplicación de la tabla de atributos:

Aplicación de atributos a ejemplo

CONTROLES Y SUS CARACTERÍSTICAS				PESO
Control 1	Tipo	Preventivo	X	25%
		Detectivo		
		Correctivo		
	Implementación	Automático		
		Manual	X	15%
Total, valoración control 1				40%
Control 2	Tipo	Preventivo		25%
		Detectivo	X	15%
		Correctivo		
	Implementación	Automático		
		Manual	X	15%
Total, valoración control 2				30%

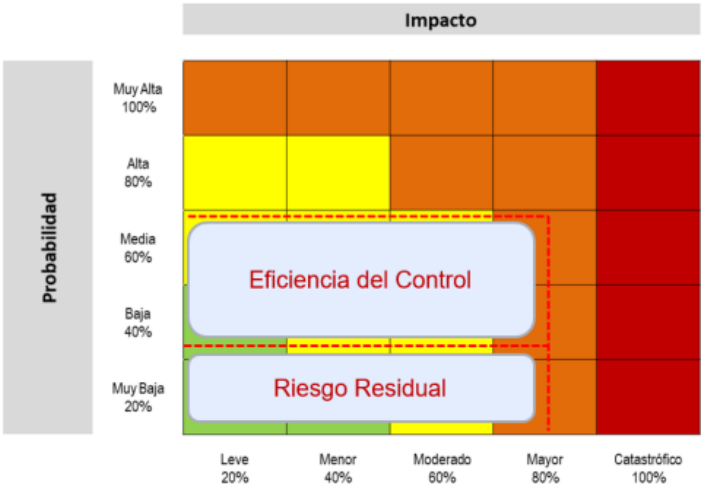
Los cálculos requeridos para la aplicación de los controles son:

Aplicación de controles para establecer el riesgo residual

RIESGO	DATOS DE PROBABILIDAD E IMPACTO		DATOS VALORACIÓN CONTROLES		CÁLCULOS
Posibilidad de afectación económica por multa y sanción del ente regulador debido a la adquisición de bienes y los servicios sin el cumplimiento de los requisitos normativos.	Probabilidad Inherente	60%	Valoración control preventivo	40%	60% * 40%= 24% 60%-24%=36%
	Valor probabilidad para aplicar 2° control	36%	Valoración control detectivo	30%	36%*30%= 10,8% 36%-10,8%=25.2%
	Probabilidad Residual	25.2%			
	Impacto Inherente	80%			
	No se tienen controles para aplicar impacto	N.A.	N.A.	N.A.	N.A.
	Impacto Residual	80%			

En la figura se observa el movimiento del mapa de calor con el ejemplo

Movimiento de la matriz de calor con el ejemplo:



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

9.6 TRATAMIENTO DEL RIESGO DE GESTIÓN, CORRUPCIÓN, SEGURIDAD DE LA INFORMACIÓN Y LAFT

Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos.

Para los riesgos **de corrupción y LAFT** la respuesta será:

EVITAR EL RIESGO. En los casos en que el riesgo es demasiado extremo se puede tomar la decisión de no realizar la actividad que lo genera. Siempre y cuando no sea obstáculo para el cumplimiento de los objetivos del proceso y de la entidad.

COMPARTIR EL RIESGO. Cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable, este puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia.

REDUCIR EL RIESGO. Para este caso se adoptan planes de acción para reducir el efecto del riesgo residual.

NOTA: Ningún riesgo de corrupción / LAFT podrá ser aceptado

Clasificación de opciones de manejo - riesgos de corrupción y LAFT

Nivel de riesgo residual	Opciones de manejo		
	Evitar	Reducir	Compartir
Bajo	NO APLICA		
Moderado		X	X
Alto	X	X	X
Extremo	X	X	X

Es importante tener en cuenta que en la definición del plan de acción se debe especificar:

- Actividad.
- Responsable
- Fecha de inicio- fecha de fin

Para los riesgos de **gestión y de seguridad de la información** la respuesta será:

EVITAR EL RIESGO. En los casos en que el riesgo es demasiado extremo se puede tomar la decisión de no realizar la actividad que lo genera. Siempre y cuando no sea obstáculo para el cumplimiento de los objetivos del proceso y de la entidad.

REDUCIR EL RIESGO. Para este caso se deben definir planes de acción para reducir el efecto del riesgo residual.

ACEPTAR EL RIESGO: Para este caso no se deben definir planes de acción.

Teniendo en cuenta los resultados de la evaluación del riesgo residual, se determinan las opciones para su tratamiento:

Clasificación de opciones de manejo riesgos de gestión y de seguridad de la información

Nivel de riesgo residual	Opciones de manejo			
	Evitar	Reducir	Aceptar	Compartir
Bajo			X	
Moderado		X		X
Alto	X	X		X
Extremo	X	X		X

Es importante tener en cuenta que en la definición del plan de acción se debe especificar:

- Actividad.
- Responsable
- Fecha de inicio – fecha de fin

9.7 MONITOREO DE LOS RIESGOS

Monitoreo de la Línea Estratégica

Los miembros de la Alta Dirección revisan y analizan el informe suministrado por la Oficina Asesora de Planeación (segunda línea de defensa) para realizar las observaciones y aportes pertinentes.

Así mismo, a través del Comité Institucional de Coordinación de Control Interno se revisan los riesgos que se han materializado con el fin tomar las decisiones a que haya lugar.

Monitoreo de la Primera Línea de Defensa

Es la actividad realizada permanentemente por los responsables de los procesos y del personal designado como enlace en la dependencia/ área en la cual deben verificar:

- Aplicación de los controles con sus respectivas evidencias de acuerdo con la periodicidad definida y tomar las acciones definidas en el mapa de riesgos en caso de observaciones o desviaciones del control.
- Implementación de las acciones para abordar riesgos con sus respectivas evidencias, las cuales deben ser registradas en el aplicativo Isolución.
- Medición del indicador cuyos resultados deben ser registrados en el aplicativo Isolución. En caso de no cumplir con la meta generar la acción correctiva.

Es importante aclarar los criterios para concluir que un riesgo se materializó, los cuales son:

- Incumplimiento de la meta del indicador.
- Afectación económica y reputacional de la entidad.

Monitoreo de la Segunda Línea de Defensa

Teniendo en cuenta que la segunda línea de defensa está conformada por la Oficina Asesora de Planeación, Área de Sistemas y responsables de los Sistemas de Gestión de Seguridad y Salud en el Trabajo y de Gestión Ambiental, el monitoreo está conformado de la siguiente manera:

Monitoreo por parte de la Oficina Asesora de Planeación: Se realizan las siguientes actividades en las frecuencias establecidas a continuación a fin de evaluar la implementación de controles, planes de acción y medición de indicadores por parte de la primera línea de defensa:

a) Mensualmente a través de la consulta en la plataforma ISOLUCION:

- Verificación de la implementación de las actividades establecidas en los planes de acción (matrices de riesgos) en las fechas establecidas.
- Cargue adecuado, completo y coherente de las evidencias de acuerdo con la información establecida en los planes de acción.
- Verificación de la información de mediciones de los indicadores y revisión de resultados para evaluar si el riesgo se ha materializado. Si el indicador se incumple se procede a generar la respectiva acción correctiva.

En caso de existir inconsistencias se da aviso por correo electrónico a los procesos para que se realicen los ajustes requeridos.

b) Trimestralmente a través de revisiones presenciales con los procesos:

- Seguimiento a la ejecución y eficacia de los controles mediante la verificación de las evidencias establecidas en los mapas de riesgos y el cumplimiento del propósito para el cual fueron creadas.
- Evaluación de la necesidad de ajustar las matrices como resultado de la implementación de controles, planes de acción y análisis de indicadores de riesgos.

El registro de esta actividad de monitoreo se realiza en la misma matriz de riesgos, en los campos creados para tal fin.

Monitoreo por parte del Área de Sistemas: A partir del reporte mensual al monitoreo que realiza el área de sistemas a los servicios tecnológicos se elabora y presenta semestralmente el informe de monitoreo relacionado con los activos de información a la Alta Dirección.

Monitoreo por parte de los responsables de otros sistemas de gestión (seguridad y salud en el trabajo, ambiental): A partir del seguimiento a las matrices de identificación de peligros/riesgos y aspectos/impactos ambientales se elabora y presenta semestralmente el informe de monitoreo de riesgos a la Alta Dirección.

Monitoreo de la Tercera Línea de Defensa

Realizado por la Oficina de Control Interno, en el cual se evalúa de manera independiente el diseño de controles y la formulación de los planes de acción definidos para los riesgos de gestión y corrupción/ LAFT.

La Oficina de Control Interno, realiza el seguimiento a la gestión de riesgos, de acuerdo con los siguientes ciclos de control (o cuando lo considere conveniente):

- Con corte a 30 de abril: El seguimiento se debe publicar en la página web de la entidaddentro de los diez (10) primeros días hábiles del mes de mayo.
- Con corte a 31 de agosto: El seguimiento se debe publicar en la página web de la entidaddentro de los diez (10) primeros días hábiles del mes de septiembre.
- Con corte a 31 de diciembre: El seguimiento se debe publicar en la página web de laentidad dentro de los diez (10) primeros hábiles días del mes de enero.

La Oficina de Control Interno determina los siguientes aspectos para concluir sobre la materialización de los riesgos:

- ✓ Si corresponde a un hecho que haya sido cuestionado por algún ente de control externo, por lo menos en una ocasión.

- ✓ Si afecta el cumplimiento de las metas y objetivos de la entidad.

10. MEDIDAS GENERALES PARA TRATAR LOS RIESGOS MATERIALIZADOS

Medidas para riesgos materializados Gestión / corrupción- LAFT

RIESGO DE GESTION /CORRUPCION – LAFT		
DETECTADO POR		
Responsables de proceso	**Oficina Asesora de Planeación**	**Oficina de Control Interno.**
Reportar de forma oportuna a la Oficina Asesora de Planeación LA MATERIALIZACIÓN **PARA RIESGOS DE CORRUPCIÓN Y LAFT** Dependiendo del alcance (normatividad asociada al hecho de corrupción o LAFT materializado), realizar la denuncia ante el ente de control respectivo.	▪ Acompañar a los procesos para actualizar el mapa de riesgos teniendo en cuenta: Aumentar el valor de probabilidad dado que el riesgo se materializó, analizar causas, revisar la calificación de controles, obtener nuevo riesgo residual, evaluar la necesidad de generar planes de tratamiento del riesgo.	▪ Informar oportunamente al Comité Institucional de Coordinación de Control Interno, al responsable del proceso (1era línea de defensa) y a la Oficina Asesora de Planeación (2da línea de defensa), acerca de los riesgos de gestión, corrupción y LAFT materializados, detectados durante las actividades de evaluación y seguimiento, reportando la situación específica, para la implementación de acciones de conformidad con la Política de Administración del riesgo. **PARA RIESGO DE CORRUPCIÓN Y LAFT** Informar a las autoridades competentes internas y/o externas a las que haya lugar con el propósito que se tomen las respectivas actuaciones.

Medidas para riesgos materializados Seguridad de información

RIESGOS DE SEGURIDAD DE LA INFORMACIÓN
DETECTADO POR
Responsable del sistema de seguridad de la información
▪ Comunicar al Oficial de seguridad ▪ Actualizar el mapa de riesgos

Medidas para riesgos materializados Seguridad y salud en el trabajo / Ambientales

RIESGOS DE SEGURIDAD Y SALUD EN EL TRABAJO RIESGOS AMBIENTALES
DETECTADO POR
Responsable del sistema de seguridad y salud en el trabajo **Responsable del sistema ambiental**
▪ Informar al Comité Paritario de Seguridad y Salud en el Trabajo, al responsable del proceso y/oSupervisor donde se materializó el riesgo, notificando a las partes interesadas ▪ Comunicar al Gestor Ambiental de la entidad. ▪ Actualizar el mapa de riesgos

APROBACIÓN

Comité Institucional de Coordinación de Control Interno - Acta Sesión Ordinaria CICCI del 20 de septiembre de 2023.