

POLÍTICA DE ADMINISTRACIÓN DE RIESGOS EN EL INSTITUTO DISTRITAL DE RECREACIÓN Y DEPORTE IDR D

Versión 5

BOGOTÁ D.C

AGOSTO DE 2022

ÍNDICE

1. OBJETIVO	3
2. ALCANCE	3
3. DEFINICIONES	3
4. MARCOS DE REFERENCIA	4
5. RIESGOS INSITUACIONALES	
6. ROLES Y RESPONSABILIDADES	4
7. APETITO AL RIESGO	8
8. TOLERANCIA AL RIESGO	8
9. ETAPAS PARA LA GESTIÓN DE RIESGOS	9
9.1. IDENTIFICACIÓN DEL RIESGO.....	9
9.2. ANÁLISIS DEL RIESGO	10
9.3. EVALUACIÓN DEL RIESGO	14
9.4. DETERMINACIÓN DEL NIVEL DE RIESGO RESIDUAL.....	17
9.5. TRATAMIENTO DEL RIESGO.....	19
9.6. MONITOREO DE LOS RIESGOS	20
10. MEDIDAS GENERALES PARA TRATAR LOS RIESGOS MATERIALIZADOS	22

ÍNDICE DE TABLAS

Tabla 1. Criterios selección mapa riesgos institucional	6
Tabla 2. Responsabilidades frente a la gestión del riesgo para la línea estratégica	7
Tabla 3. Responsabilidades frente a la gestión del riesgo para la primera línea de defensa	8
Tabla 4. Responsabilidades frente a la gestión del riesgo para la segunda línea de defensa	9
Tabla 5. Responsabilidades frente a la gestión del riesgo para la tercera línea de defensa	10
Tabla 6. Criterios para definir el nivel de probabilidad	13
Tabla 7. Criterios para definir el nivel de impacto	14
Tabla 8. Criterios y elementos para calcular impacto económico	14
Tabla 9. Criterios y elementos para calcular impacto económico	16
Tabla 10 Criterios para calificar el impacto – riesgos de corrupción	17
Tabla 11. Variables para el diseño de controles	19
Tabla 12. Evaluación de controles	22

Tabla 13. Aplicación de atributos a ejemplo	24
Tabla 14. Aplicación de controles para establecer el riesgo residual.....	25
Tabla 15. Clasificación de opciones de manejo.....	27
Tabla 16. Medidas para riesgos materializados Gestión / corrupción	30
Tabla 17. Medidas para riesgos materializados Seguridad de información	31
Tabla 18. Medidas para riesgos materializados Seguridad y salud en el trabajo / Ambientales ..	31

ÍNDICE DE FIGURAS

Figura 1. Redacción del riesgo	12
Figura 2. Mapa de calor (matriz de calificación)	18
Figura 3. Movimiento en la matriz de calor acorde con el tipo de control.	21
Figura 4. Mapa de calor riesgos de corrupción	23
Figura 5. Movimiento de la matriz de calor con el ejemplo:	25
Figura 6. Opciones para abordar los riesgos mediante acciones	26

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 y corrupción 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

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.

5. MAPA DE RIESGOS INSTITUCIONAL

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:

Tabla 1. 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	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 gestión del riesgo 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 una de estos roles:

Tabla 2. Responsabilidades frente a la gestión del riesgo para la línea estratégica

LÍNEA ESTRATÉGICA		
RESPONSABLES		
<p>Alta Dirección (Nota: Los integrantes de la Alta Dirección son los que hacen parte del Comité Institucional Gestión y Desempeño los cuales se mencionan en el artículo 3° de la Resolución 265 de 2020)</p>	<p>Comité Institucional de Coordinación de Control Interno (CICCI)</p>	
<p>Responsabilidades frente al riesgo</p>	<ul style="list-style-type: none"> ▪ 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 	<ul style="list-style-type: none"> ▪ Someter a aprobación del representante legal la política de administración de riesgos y hacer seguimiento, en especial a la prevención y detección de fraude y mala conducta
	<ul style="list-style-type: none"> ▪ 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. 	<ul style="list-style-type: none"> ▪ 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 la repetición de los mismos

Tabla 3. Responsabilidades frente a la gestión del riesgo para la primera línea de defensa

PRIMERA LINEA	
Responsables	
Responsables de los procesos	
Responsabilidades frente al riesgo	<ul style="list-style-type: none"> ▪ 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. ▪ Implementar los controles establecidos para reducir o mitigar los riesgos de gestión y de corrupción ▪ Documentar en los procedimientos los controles para abordar los riesgos de gestión. ▪ Tratar los riesgos residuales de gestión y corrupción, cuando aplique, mediante la definición de planes e implementación oportuna de los mismos con el fin de reducir su 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	
	<ul style="list-style-type: none"> ▪ 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 “<i>Baja ejecución de metas de los proyectos de inversión</i>”. 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.

Tabla 4. Responsabilidades frente a la gestión del riesgo para la segunda línea de defensa

SEGUNDA LINEA	
Responsables	
Oficina Asesora de Planeación	Responsable del Sistema de Gestión de Seguridad y Salud en el Trabajo Responsable del Sistema Ambiental
Responsabilidad es frente al riesgo	<ul style="list-style-type: none"> ▪ Orientar a la línea estratégica en la definición y actualización de la política de administración de riesgos en el IDR. ▪ Coordinar con los procesos la actualización de 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. ▪ 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
	<ul style="list-style-type: none"> ▪ 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. ▪ 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 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.

Tabla 5. Responsabilidades frente a la gestión del riesgo para la tercera línea de defensa

T E R C E R A L Í N E A	
Responsables	
Oficina de Control Interno	
Responsabilidades frente al riesgo	<ul style="list-style-type: none"> ▪ 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 ▪ Evaluar de manera independiente y objetiva los controles de la segunda línea de defensa para asegurar su efectividad y cobertura; así mismo, evaluar los controles de primera línea de defensa que no se encuentren cubiertos y los que inadecuadamente son cubiertos por la segunda línea de defensa. ▪ 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 las responsabilidades en materia de riesgos. ▪ Formar a la alta dirección y a todos los niveles de la entidad sobre las responsabilidades en materia de riesgos. ▪ Informar los hallazgos y proporcionar recomendaciones de forma independiente.

7. APETITO DEL RIESGO

El apetito al 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 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 y seguridad de la información) es cero (0%).

9. ETAPAS PARA LA GESTIÓN DE RIESGOS

9.1. IDENTIFICACIÓN DEL RIESGO:

Los riesgos identificados deben dar cuenta de los siguientes factores:

- Los eventos adversos que puedan presentarse e inciden en el cumplimiento de los objetivos estratégicos y del proceso.
- Las actividades que hacen parte del flujo del proceso y que son vulnerables creando amenazas frente al cumplimiento del objetivo del proceso.
- El análisis de las PQRS
- Cambios en la normatividad
- Modificaciones en activos de información
- Evaluaciones realizadas por entes externos de control.
- Los resultados de las auditorías de control interno, así mismo cuando existan informes emitidos por la Oficina de Control Interno (Tercera línea de defensa), con observaciones y recomendaciones en el tema a fin de realizar los ajustes a que haya lugar.

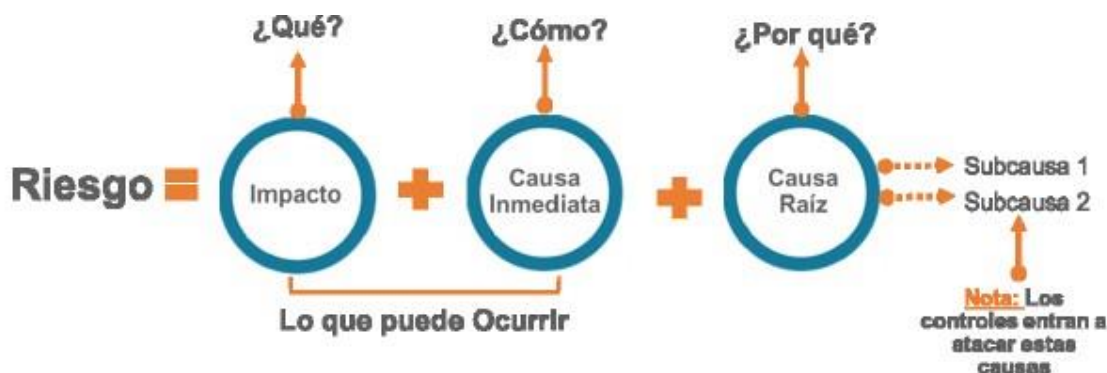
El IDRD actualiza las matrices de riesgos de gestión, corrupción y seguridad de la información teniendo en cuenta el análisis de los factores anteriormente descritos cuya periodicidad depende de la ocurrencia de estos. En todo caso, la frecuencia de actualización no puede superar un año y se hará en el primer trimestre de la vigencia.

NOTA: En el mapa de riesgos se lleva la trazabilidad de las revisiones y cambios según corresponda.

Otro factor para tener en cuenta es el análisis del contexto externo, interno cuyo análisis se realiza 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.

Los riesgos se describen a través de la siguiente estructura:

Figura 1. Redacción del riesgo



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 organización la materialización del 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 concurren los componentes de su definición, así: Acción u omisión + Uso del poder + Desviación de la gestión de lo público + El beneficio privado.

9.2. ANÁLISIS DEL RIESGO

9.2.1 RIESGOS DE GESTIÓN Y 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. La Tabla 6 presenta los criterios para definir el nivel de probabilidad

Tabla 6. 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 reputacional conforme a los criterios establecidos en la tabla 7.

Tabla 7. 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

Para realizar el cálculo de la afectación económica, se utilizarán los siguientes criterios definidos en la versión 2018 de la Guía de administración del riesgo del DAFP:

- Afectación por ejecución presupuestal
- Pagos por sanciones económicas
- Indemnizaciones a terceros
- Sanciones por incumplimientos de tipo legal
- Vulneraciones a la información
- Fallas en la prestación del servicio

Para facilitar el cálculo y definir el rango de la afectación económica, a continuación se presentan los parámetros a tener en cuenta por cada criterio: Es de anotar que el cálculo es un referente y no necesariamente podrá ser una cifra exacta.

Tabla 8. Criterios y elementos para calcular impacto económico

Criterio	Elementos para realizar el cálculo
Afectación por ejecución presupuestal	<ul style="list-style-type: none"> • Normativa relacionada con la reducción del presupuesto de Gastos de funcionamiento o de apropiaciones de inversión cuando las reservas constituidas para ellos superen el porcentaje definido en la norma con relación al presupuesto del año inmediatamente anterior. • Afectación en la apropiación presupuestal por bajo recaudo de rentas o ingresos. • Históricos de presupuesto no ejecutado • Históricos de afectación presupuestal por retrasos de obra

Criterio	Elementos para realizar el cálculo
Pagos por sanciones económicas	Normativa relacionada con la aplicación de multas por no responder con oportunidad y/o calidad solicitudes de información de entes de control.
Indemnizaciones a terceros	<p>Para este caso, se podrá acudir a la información que reporta el IDR en el Sistema de Información de Procesos Judiciales de la Secretaría Jurídica de la Alcaldía Mayor de Bogotá.</p> <p>Teniendo en cuenta que las indemnizaciones a terceros están relacionadas con daño emergente y lucro cesante (accidentes de trabajo, despidos injustificados, incumplimientos a terceros), se puede tomar la base histórica que pagos a terceros para determinar el mínimo, el máximo o el promedio de pagos por indemnización efectuados.</p>
Sanciones por incumplimientos de tipo legal	<p>Se debe analizar si la entidad reporta información a entidades que realicen labores de Inspección, Vigilancia y Control (Superintendencias). Estas entidades tienen definidas las sanciones económicas a pagar en caso de que la información no sea reportada con calidad y/o oportunidad.</p> <p>Por otra parte, se deben tener en cuenta los lineamientos de la Dirección de Impuestos y Aduanas Nacionales DIAN, para el cálculo de las multas a pagar por no suministrar información tributaria o enviarla con errores.</p>
Vulneraciones a la información	<p>Para calcular la afectación económica de esta variable se puede tomar la información histórica que exista en la entidad, relacionada con pérdida de expedientes, ataques o virus informáticos, así mismo, se puede consultar la base de datos de activos de información de la entidad analizando la criticidad de determinado activo y el valor de este.</p> <p>Por otra parte, se puede acudir a los históricos sobre recuperación de información física o virtual, teniendo en cuenta el costo de recuperación de un activo de información como lo es la reconstrucción de un expediente físico, o la puesta en operación de bases de datos que se encuentran en sistemas de información.</p> <p>En caso de que no se tengan registros históricos, se puede realizar el cálculo del valor actual del activo de información.</p> <p>También se podrá realizar el cálculo analizando la afectación económica por no tener el activo de información para la prestación del servicio, de acuerdo con el promedio de ingresos que la entidad dejó de percibir por no poder ejecutar los servicios prestados.</p>
Fallas en la prestación del servicio	<p>La afectación económica por esta variable puede calcularse por los recursos que deje de percibir el Instituto a causa de fallas en los sistemas de información dedicados al préstamo de parques o escenarios.</p> <p>Se puede tomar la base histórica de pagos realizados al Instituto para determinar el mínimo, el máximo o el promedio de ingresos que se obtienen en un periodo de tiempo definido (diario o mensual) con el fin de determinar el impacto económico por no poder prestar el servicio ofrecido.</p> <p>La afectación económica también puede calcularse con los bienes devolutivos o de consumo que se encuentren en parques y/o escenarios del Instituto cuya pérdida genere afectación en el servicio. Para esto se puede recurrir a promedios históricos relacionados con valores asociados con pérdidas de bienes.</p>

Cálculo del impacto:

Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, 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

9.2.2. RIESGOS DE CORRUPCIÓN:

La tabla 9 presenta los criterios para definir el nivel de **probabilidad**:

Tabla 9. 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.

El **análisis de impacto** se realiza teniendo en cuenta solamente los niveles Moderado, Mayor y Catastrófico, dado que estos riesgos siempre serán significativos y no pueden ser aceptados. En este caso, se utilizan los criterios definidos en la tabla 10.

Tabla 10 Criterios para calificar el impacto – riesgos de corrupción

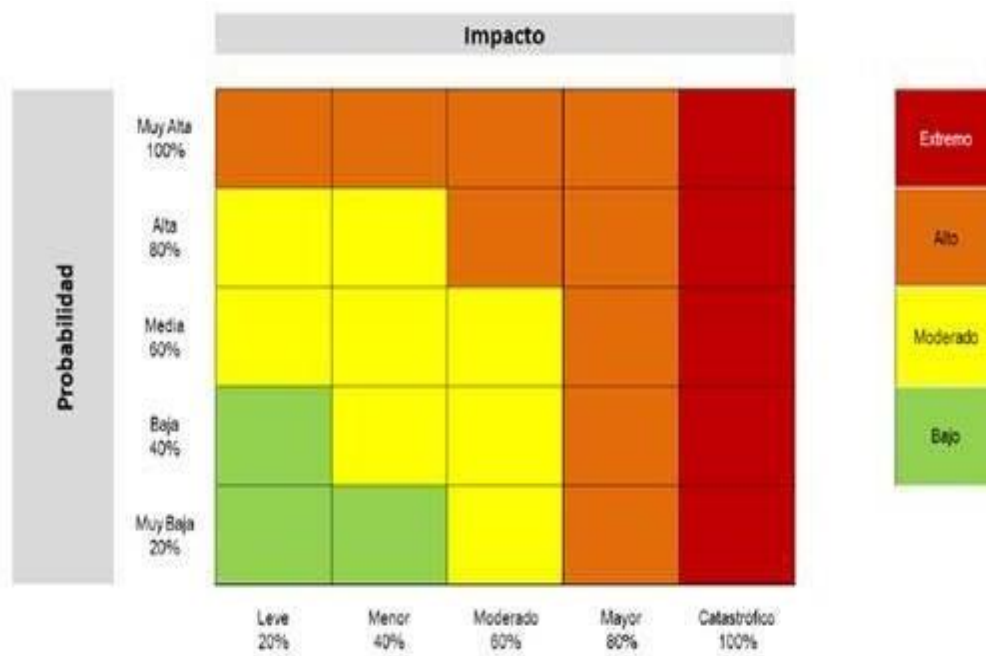
No.	Pregunta: Si el riesgo de corrupción se materializa podría...	Respuesta	
		Si	No
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de misión de la entidad?		
4	¿Afectar el cumplimiento de la misión del 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?		
<p>Si se responde afirmativamente de 1 a 5 preguntas, el impacto es Moderado (genera medianas consecuencias para la entidad).</p> <p>Si se responde afirmativamente de 6 a 11 preguntas, el impacto es Mayor (genera altas consecuencias para la entidad).</p> <p>Si se responde afirmativamente de 12 a 19 preguntas, el impacto es Catastrófico (genera consecuencias desastrosas para la entidad).</p>			

Una vez se obtenga el impacto y la probabilidad para cada riesgo identificado, se ubican las calificaciones respectivas en la fila y columnas correspondientes sobre el mapa de calor y se establece el punto de intersección entre ambas, el cual corresponde al nivel de riesgo inherente; es decir, el riesgo que enfrenta la entidad en ausencia de controles. La entidad utiliza mapas de calor con 5 niveles de calificación de impacto y 5 niveles de calificación de probabilidad, como se ilustra a continuación en la figura 2.

Para los riesgos de corrupción, únicamente aplican los niveles Moderado, Alto y Extremo

Figura 2. Mapa de calor (matriz de calificación)



9.3. EVALUACIÓN DEL RIESGO DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DE LA INFORMACIÓN

En esta etapa se confrontan los resultados del análisis del riesgo inherente frente a los controles establecidos, con el fin de determinar el nivel de riesgo final (riesgo residual). La evaluación del riesgo requiere el diseño y la valoración de los controles.

Los controles son aquellas medidas orientadas a reducir o mitigar el riesgo. Para la valoración de los controles se debe tener en cuenta:

- La identificación de los controles se debe realizar a cada riesgo a través de entrevistas con los líderes de proceso y servidores expertos en su quehacer.
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de sus equipos de trabajo.

Para una adecuada redacción del control se propone la estructura que se presenta en la tabla 11.

Tabla 11. Variables para el diseño de controles

Variable	Descripción
Responsable	<p>Persona asignada para ejecutar el control. Debe tener la autoridad, competencias y conocimientos para ejecutar el control dentro del proceso.</p> <p>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.</p>
Periodicidad	<p>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.</p> <p>Pueden existir control 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.</p>
Propósito	<p>El control debe tener un propósito que indique para qué se realiza, y que ese propósito conlleve a prevenir las causas que generan el riesgo. Se deben utilizar verbos que indiquen actividades específicas de control. Entre otros, se debe redactar el control con los siguientes ejemplos de verbos:</p> <ul style="list-style-type: none"> • Verificar • Validar • Conciliar • Comparar • Revisar • Cotejar <p>No se deben utilizar verbos como:</p>

	<ul style="list-style-type: none"> • Elaborar • Diseñar • Programar • Solicitar • Divulgar
Cómo se realiza la actividad de control	El control debe indicar detalladamente el cómo se realiza
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 se clasifican en:

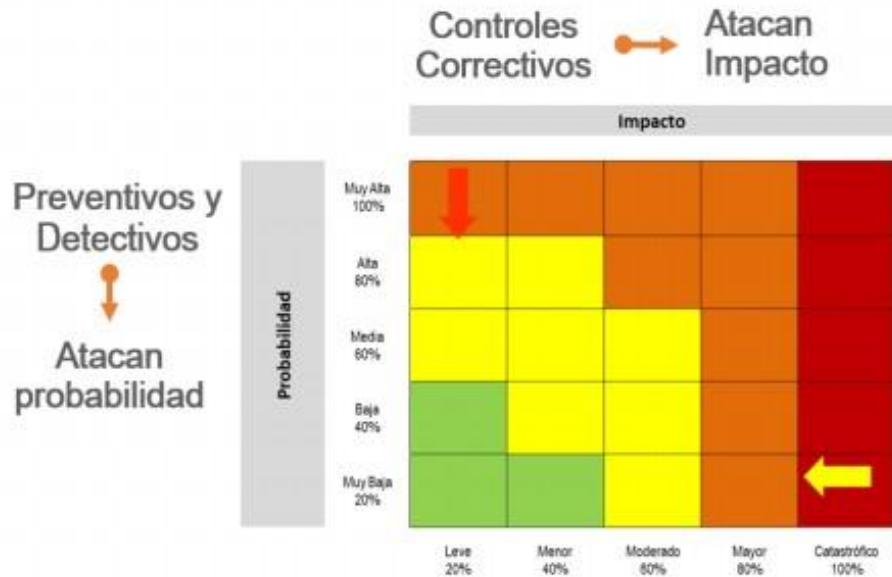
Preventivos. Contrarrestan las causas del riesgo para evitar que ocurran y deben ser aplicados antes de que se realice la actividad que origina el riesgo.

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

Correctivos. Actúan posterior a la materialización el riesgo.

Los controles preventivos y detectivos reducen la probabilidad y los correctivos, el impacto en el sentido que presenta la figura 3.

Figura 3. 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 valoración de los controles para la mitigación de los riesgos se realiza mediante la evaluación del diseño de estos establecidos en la tabla 12.

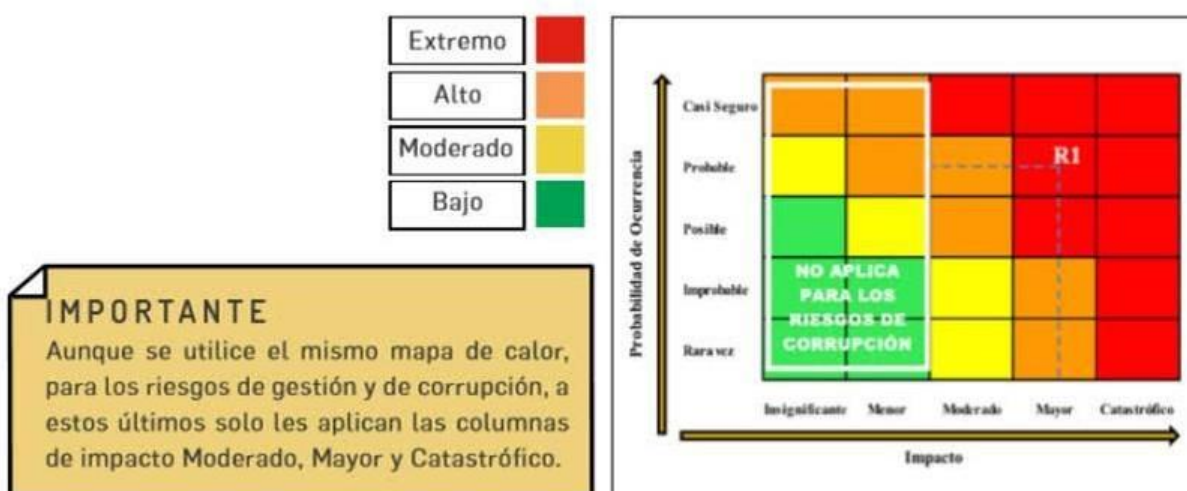
Tabla 12. Evaluación de controles

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

*Los atributos informativos solo permiten darle formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, estos no tienen ninguna incidencia directa de su efectividad.

Para los riesgos de corrupción, el análisis de impacto se realizará teniendo en cuenta solamente 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. Tal y como se muestra en la siguiente figura:

Figura 4. Mapa de calor riesgos de corrupción



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

9.4. DETERMINACIÓN DEL NIVEL DE RIESGO RESIDUAL PARA GESTIÓN, CORRUPCIÓN Y SEGURIDAD DE LA INFORMACIÓN

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.

En la tabla 13 se presenta la aplicación de la tabla de atributos:

Tabla 13. 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%

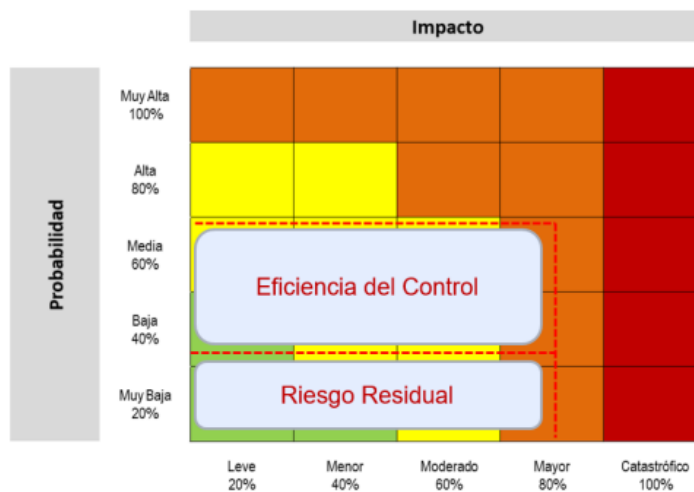
Los cálculos requeridos para la aplicación de los controles se presentan en la tabla 14.

Tabla 14. 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%
	Valor probabilidad para aplicar 2° control	36%	Valoración control detectivo	30%	60%-24%=36%
	Probabilidad Residual	25.2%			36%*30%= 10,8%
	Impacto Inherente	80%			36%-10,8%=25.2%
	No se tienen controles para aplicar impacto	N.A.	N.A.	N.A.	N.A.
	Impacto Residual	80%			

En la figura 5 se observa el movimiento del mapa de calor con el ejemplo

Figura 5. Movimiento de la matriz de calor con el ejemplo:

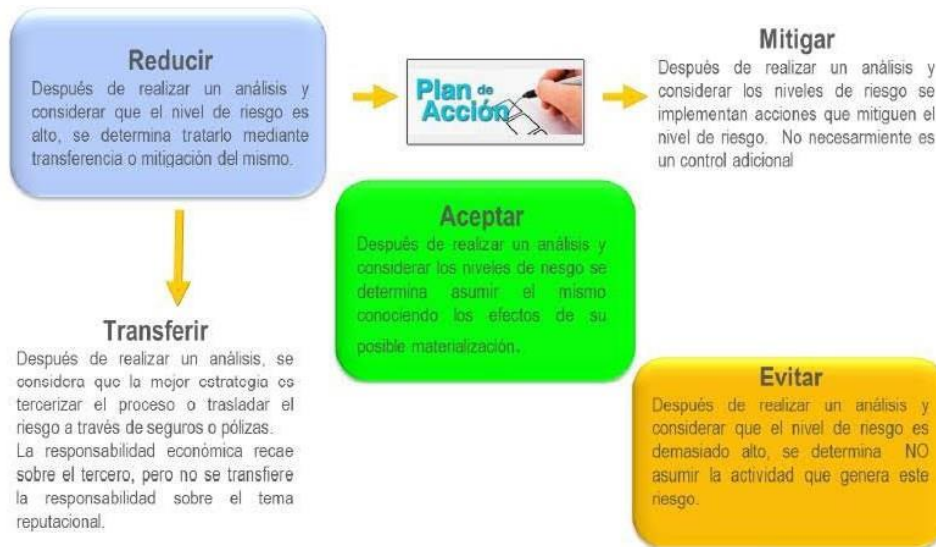


Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

9.5. TRATAMIENTO DEL RIESGO DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DE LA INFORMACIÓN

El tratamiento del riesgo involucra la selección de una o más opciones para abordar los riesgos y la definición de un plan de acción como se indica en la figura 6.

Figura 6. Opciones para abordar los riesgos mediante acciones



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

Teniendo en cuenta los resultados de la evaluación del riesgo residual, se determinan las opciones para su tratamiento según lo definido en la tabla 15.

NOTA: Para los riesgos de corrupción la respuesta será evitar o reducir. - **“NO ACEPTAR”**

Tabla 15. Clasificación de opciones de manejo

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

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

- ❖ Actividad.
- ❖ Responsable
- Fecha de implementación

9.6. MONITOREO DE LOS RIESGOS

9.6.1 Monitoreo de la Línea Estratégica

Es la actividad realizada por la Alta Dirección de la entidad, en el marco del Comité Institucional de Coordinación de Control Interno, mediante la cual se evalúa 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 tomar de tomar las decisiones a que haya lugar.

9.6.2 Monitoreo de la Primera Línea de Defensa

Es la actividad realizada por los responsables de los procesos permanentemente y del personal designado como enlace en la dependencia/ área en la cual deben verificar que se estén ejecutando los controles y los planes de acción establecidos para la mitigación y tratamiento de los riesgos respectivamente.

El monitoreo debe quedar registrado mensualmente en el instrumento establecido por la Oficina Asesora de Planeación.

El monitoreo incluye:

- ✓ Contar oportunamente con las evidencias completas de los controles establecidos de acuerdo con la periodicidad definida
- ✓ Tomar las acciones definidas en el mapa de riesgos en caso de observaciones o desviaciones del control
- ✓ Reportar oportunamente en Isolución el seguimiento al plan de acción de acuerdo con las fechas establecidas, adjuntando las evidencias correspondientes
- ✓ Reportar oportunamente en Isolución las mediciones de los indicadores definidos en el mapa verificando el cumplimiento de la meta, y si es del caso, generar la acción correctiva tal y como lo establece la tolerancia del riesgo definido en el ítem 8 de este documento.

9.6.3 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: A partir de la información reportada por la primera línea de defensa en el instrumento de monitoreo, y teniendo en cuenta la gestión realizada por la Oficina Asesora de Planeación para la gestión de riesgos en el Instituto, se elaborará y presentará cuatrimestralmente el informe de monitoreo de riesgos a la Alta Dirección.

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 elaborará y presentará 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): Efectuar el seguimiento a la matriz de identificación de peligros, riesgos, aspectos ambientales e impactos propios de cada sistema. Se elaborará y presentará semestralmente el informe de monitoreo de riesgos a la Alta Dirección.

Monitoreo riesgos contractuales: La Subdirección de Contratación es la encargada de dar los lineamientos para realizar el monitoreo a los riesgos del proceso de contratación de acuerdo con las indicaciones establecidas en el Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación expedido por Colombia Compra Eficiente.

9.6.4 Monitoreo de la Tercera Línea de Defensa

Es la etapa realizada por la Oficina de Control Interno, donde se evalúa de manera independiente la gestión de riesgos, verificando la efectividad de los controles, mediante actividades de evaluación y seguimiento. Esta evaluación tiene los siguientes propósitos:

Valorar de forma independiente el diseño de los controles y la formulación de los planes de acción y planes de contingencia definidos para los riesgos de gestión y corrupción.

La Oficina de Control Interno, realiza el seguimiento a la gestión de riesgos, de acuerdo con los siguientes ciclos de control:

- Con corte a 30 de abril: El seguimiento se debe publicar en la página web de la entidad dentro 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 entidad dentro 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 la entidad dentro de los diez (10) primeros hábiles días del mes de enero.

No obstante, lo anterior la Oficina de Control Interno podrá realizar seguimientos adicionales cuando lo considere conveniente.

Entendiendo que la estructura del MECI, se concreta en la 7ª Dimensión del MIPG, la Oficina de Control Interno en su rol de tercera línea como evaluador independiente, se pronunciará en términos de riesgos y su posible materialización, teniendo en cuenta los siguientes aspectos:

- ✓ Si la Oficina de Control Interno en desarrollo de los roles de evaluación a la gestión del riesgo, evaluación y seguimiento establecidos en el Decreto 648 de 2017, identifica la ocurrencia del riesgo o posible materialización del mismo.
- ✓ Si la ocurrencia del riesgo corresponde a un hecho que haya sido cuestionado por algún Ente de control externo, por lo menos en una ocasión.
- ✓ Si la Oficina de Control Interno identificó que la ocurrencia del riesgo afecta el cumplimiento de las metas y objetivos de la entidad

10. MEDIDAS GENERALES PARA TRATAR LOS RIESGOS MATERIALIZADOS

Tabla 16. Medidas para riesgos materializados Gestión / corrupción

RIESGO DE GESTION / CORRUPCION		
DETECTADO POR		
Responsables de proceso	Oficina Asesora de Planeación	Oficina de Control Interno.
<ul style="list-style-type: none"> ▪ Reportar de forma oportuna a la Oficina Asesora de Planeación mediante el instrumento de monitoreo para actualizar en mesa de trabajo el mapa de riesgos. <p>PARA RIESGOS DE CORRUPCIÓN:</p> <p>Dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante el ente de control respectivo.</p>	<ul style="list-style-type: none"> ▪ 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 en caso de que la causa haya sido la no implementación de éstos, obtener nuevo riesgo residual, evaluar la necesidad de generar planes de tratamiento del riesgo. 	<ul style="list-style-type: none"> ▪ Informar oportunamente al Comité Institucional de Coordinación de Control Interno, al responsable del proceso (1^{era} línea de defensa) y a la Oficina Asesora de Planeación (2^{da} línea de defensa), acerca de los riesgos de gestión y/o corrupción 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. <p>PARA RIESGO DE CORRUPCIÓN:</p> <p>Informar a las autoridades competentes internas y/o externas a las que haya lugar con el propósito que se tomen las respectivas actuaciones.</p>



Tabla 17. Medidas para riesgos materializados Seguridad de información

RIESGOS DE SEGURIDAD DE LA INFORMACIÓN
DETECTADO POR
Responsable del sistema de seguridad de la información
<ul style="list-style-type: none"> ▪ Comunicar al Oficial de seguridad ▪ Informar a la OAP acerca de los riesgos materializados ▪ Actualizar el mapa de riesgos

Tabla 18. 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
<ul style="list-style-type: none"> ▪ Informar al Comité Paritario de Seguridad y Salud en el Trabajo, al jefe inmediato y/o Supervisor, acerca de los riesgos materializados, notificando a las partes interesadas ▪ Comunicar al Gestor Ambiental de la Entidad, acerca de los riesgos materializados. notificando a las partes interesadas. ▪ Actualizar el mapa de riesgos

APROBACIÓN

ELABORÓ	REVISÓ	APROBÓ
 Martha Rodríguez Martínez Jefe Oficina Asesora de Planeación	Comité Institucional de Coordinación de Control Interno	 Blanca Inés Durán Hernández Directora General
		FECHA DE APROBACIÓN
		Acta Sesión Extraordinaria CICC del 30 de agosto de 2022