Empresa de Desarrollo Sostenible

RESOLUCIÓN No. 108

5 JUN 2022

"POR MEDIO DEL CUAL SE ACTUALIZA LA POLÍTICA DE ADMINISTRACIÓN DEL RIESGO DE LA EMPRESA DE DESARROLLO SOSTENIBLE DEL ORIENTE – EDESO - RIONEGRO"

La Gerente de la Empresa de Desarrollo Sostenible del Oriente de Rionegro, en uso de sus atribuciones legales y especialmente las conferidas en el artículo 315 Constitucional, la Ley 909 de 2004, y el artículo 29 de la ley 1551 de 2012,

CONSIDERANDO:

Mediante el artículo 209 de la Constitución Política se establece que la administración pública tendrá un control interno. El artículo 269 determina la obligación de diseñar y aplicar el control interno en las entidades del estado.

Que la Ley 87 de 1993 establece que la Entidad debe disponer de procesos de planeación y mecanismos adecuados para el diseño y desarrollo organizacional de acuerdo a su naturaleza y características.

Que mediante Decreto 2145 de 1999 se dictan normas sobre el Sistema Nacional de Control Interno de las Entidades y Organismos de la Administración Pública del orden nacional y territorial y se dictan otras disposiciones.

Que el Decreto 1499 de 2017 absorbe los dos Sistemas de Gestión y el Modelo Estándar de Control Interno y crea el Modelo Integrado de Planeación y Gestión – MIPG donde se debe desarrollar la Política de Administración del riesgo en la dimensión de Control Interno.

En mérito de lo expuesto,

RESUELVE:

ARTÍCULO PRIMERO: Actualizar la Política de Administración del Riesgo de la Empresa de Desarrollo Sostenible – EDESO, Rionegro, Antioquia, donde se adicionan los riesgos de corrupción y riesgos de seguridad de la información integrados todos en una sola política de administración del riesgo y en una sola

matriz de administración del riesgo por procesos.

ARTÍCULO SEGUNDO: DEFINICIÓNES:

Riesgo: Posibilidad de que se produzca un contratiempo o una desgracia, de que alguien o algo sufra perjuicio o daño..

Modelo de las tres líneas de defensa: Modelo que permite la administración de riesgos y controles, esto se logra a través de **establecer funciones y deberes relacionados entre los diferentes frentes de la administración de riesgos y** asegurar que no se realicen controles o esfuerzos duplicados a cargo de los diversos actores de la Administración del Riesgo.

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

Apetito de Riesgo: Nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito puede ser diferente para los distintos tipos de riesgos que la entidad debe gestionar.

Capacidad de riesgo: Máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.

Causa: Aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

Causa Inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

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

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

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

Control: Medida que permite reducir o mitigar un riesgo.

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

Factores de riesgo: Son las fuentes generadoras de riesgos.

Integridad: Propiedad de exactitud y completitud.

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

Nivel de riesgo: 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. Pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.

Probabilidad: Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

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

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

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

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

Riesgo Residual: El resultado de aplicar la efectividad de los controles al riesgo inherente.

Tolerancia del riesgo: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.

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

ARTÍCULO TERCERO: MODIFICACIÓN. La Política de ADMINISTRACIÓN DEL RIESGO podrá ser modificada y actualizada, de conformidad con las disposiciones legales existentes.

ARTÍCULO CUARTO: VIGENCIA. La presente Resolución rige a partir de la fecha y deroga todos los actos que le sean contrarios.

ARTÍCULO QUINTO: PUBLICACIÓN. Ordenar la publicación de la mencionada Política, a través de los mecanismos previstos en la Ley 1712 de 2014.

Dado en Rionegro, a los

¡COMUNÍQUESE Y CÚMPLASE!

MARTHA PATRICIA CORREA TABORDA
Gerente

Proyectó y actualizó: Dr. Mauricio Garcia Escobar, Jefe de Control Interno
Reviso: Diego Ocazionez, Secretario General.

POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

INTRODUCCIÓN

La Empresa de desarrollo Sostenible del Oriente – EDESO – Rionegro, en cumplimiento de sus funciones, fortalece el Sistema de Control Interno para proveer seguridad razonable para el logro de los objetivos estratégicos institucionales, dando cumplimiento a la normatividad vigente, mediante la gestión oportuna de los riesgos y la efectividad de los controles.

Así mismo, la Empresa está comprometida con establecer y mantener una Política de Administración del Riesgo Interno, alineada a la planeación estratégica y operatividad en los procesos, en el cual todos los funcionarios y contratistas apliquen los criterios definidos en esta política por procesos, para mantener y ejercer los controles efectivos y eficientes a los riesgos y evitar que se materialicen.

La empresa se encuentra en un nivel incipiente de implementación de la política de administración del riesgo y se deben determinar los roles y responsabilidades conjuntas desde la estrategia de las líneas de defensa.

JUSTIFICACION

La Política de Administración del Riesgo es desarrollada en el marco del Modelo Integrado de Planeación y Gestión-MIPG en la séptima dimensión "Control Interno" que se desarrolla a través del Modelo Estándar de Control Interno – MECI en el componente de Evaluación de Riesgos, el cual se desarrolla a través de la estrategia de las líneas de defensa (Estratégica, Primera Línea, Segunda Línea y Tercera Línea).

OBJETIVO

Establecer los lineamientos generales e instrumentos requeridos para la administración y control de los riesgos que puedan afectar el logro de los objetivos institucionales y de proceso, con el propósito de minimizar posibles desviaciones y efectos nocivos para la entidad.

ALCANCE

Los lineamientos de esta política de administración de riesgos, deben aplicarse por parte de los responsables de acuerdo con su rol definido en las líneas de defensa de manera transversal, a los objetivos estratégicos, procesos, planes, programas y proyectos de la Entidad, desde la identificación del contexto del riesgo hasta el seguimiento, tratamiento y comunicación de la información resultante de la administración de este; desarrollado mediante el manual vigente "Metodología para la Administración de Riesgos de Gestión, Corrupción y Seguridad de la Información"

CONDICIONES GENERALES

Una vez realizada la fase de valoración del riesgo después de definidos los controles se debe aplicar la opción de tratamiento. Esto se define a partir de datos cuantitativos del nivel de riesgo residual, de la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto de este y la relación costo-beneficio de las medidas de tratamiento.

DEFINICIONES O GLOSARIO

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

- **Apetito de Riesgo:** Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debeNo desea gestionar.

- **Capacidad de riesgo:** Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.

- **Causa:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

- **Causa Inmediata:** Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

- **Causa Raíz:** Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

- **Confidencialidad:** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

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

- **Control:** Medida que permite reducir o mitigar un riesgo.

- **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.

- **Factores de riesgo:** Son las fuentes generadoras de riesgos.

- **Integridad:** Propiedad de exactitud y completitud.

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

- **MECI:** Modelo Estándar de Control Interno.

- **MIPG:** Modelo Integrado de Planeación y Gestión.

- **Nivel de riesgo:** Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo poder ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.

- **Probabilidad:** Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

- **Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a

eventos potenciales. Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

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

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

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

- **Riesgo Residual:** El resultado de aplicar la efectividad de los controles al riesgo inherente.

- **Tolerancia del riesgo:** Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.

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

DESCRIPCIÓN

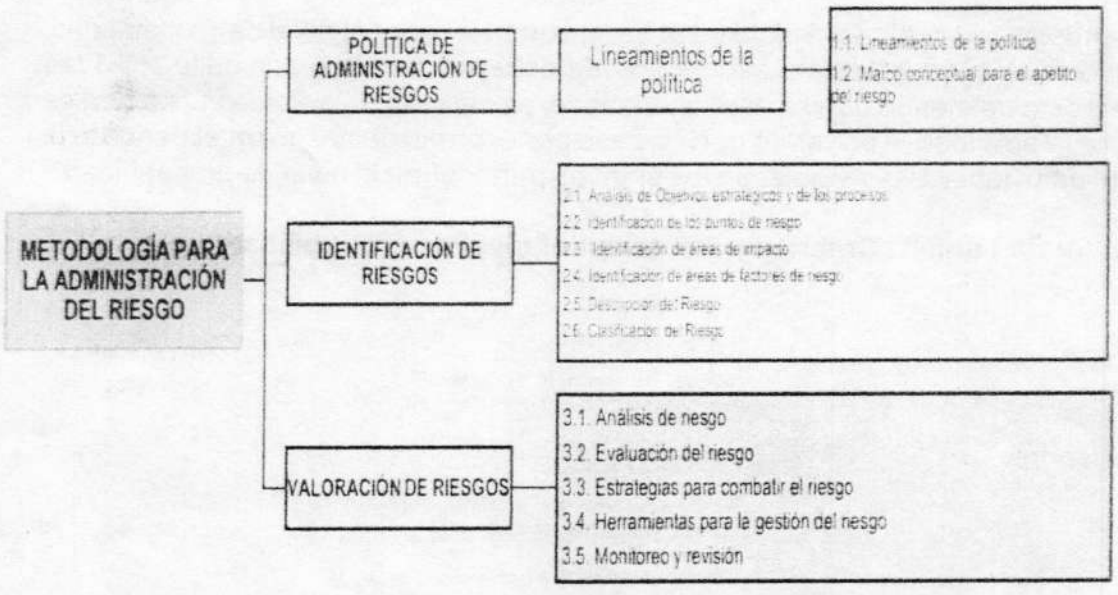
La Empresa se compromete con la asignación de los recursos, condiciones, lineamientos, responsabilidades e instrumentos necesarios para la adecuada administración de los riesgos, asegurando de este modo y de manera razonable, el logro de sus objetivos e iniciativas, implementando las acciones necesarias para una efectiva administración del riesgo, que permitan su identificación, valoración, monitoreo, tratamiento y comunicación en coherencia con los roles que desempeña cada una de las líneas de defensa.

a. Estructura para la Administración de Riesgos

i. Metodología a utilizar

Comprende, los lineamientos de la política de administración de riesgos, el marco conceptual para el apetito del riesgo, la identificación del riesgo y la valoración del riesgo. El desarrollo de las diferentes etapas que se presentan a continuación, se describe en el manual vigente de " Metodología para la Administración de Riesgos de Gestión, Corrupción y Seguridad de la Información".

Ilustración 1: Gestión de los riesgos



ii. Herramientas para la Gestión del Riesgo

La Empresa cuenta con el formato "Matriz Mapa de Riesgos", como herramienta asociada al Manual "Metodología para la Administración de Riesgos de Gestión, Corrupción y Seguridad de la Información". En este se gestionan los riesgos, desde la identificación de los factores de riesgos hasta el respectivo seguimiento de acuerdo con la periodicidad establecida.

iii. Análisis de Riesgos

En el análisis de riesgos se establece la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (Riesgo Inherente).

- **Determinar la probabilidad**

Por probabilidad se entiende la posibilidad de ocurrencia del riesgo, la probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Teniendo en cuenta lo explicado en el punto anterior sobre el nivel de probabilidad, la exposición al riesgo estará asociada a la frecuencia de ejecución de la actividad generadora del riesgo que se esté analizando, es decir, al número de veces que se ejecuta la actividad, y por ende que se pasa por el punto de riesgo en el periodo de 1 año, en la tabla 1 se establecen los criterios para definir el nivel de probabilidad.

Tabla 1. Criterios para definir el nivel de probabilidad

	Frecuencia de La Actividad	Probabilidad
Muy baja	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces al año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces al año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 25 a 500 veces al año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 501 veces al año y máximo 5000 veces al año	80%
Muy alta	La actividad que conlleva el riesgo se ejecuta mas de 5001 veces al año	100%

- **Análisis de la probabilidad (Riesgo de corrupción)**

Se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de frecuencia o factibilidad, donde frecuencia implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; factibilidad implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo,

se trata en este caso de un hecho que no se ha presentado pero es posible que suceda.

Tabla 2. Criterios para calificar la probabilidad (Riesgos de corrupción)

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
5	Casi seguro		
4	Probable		
3	Posible		
2	Improbable		
1	Rara vez		

- **Determinar la probabilidad riesgos de seguridad digital**

Para esta etapa se asociarán las tablas de probabilidad e impacto definidas para los riesgos de gestión.

- **Calificación del Impacto**

Riesgos de Gestión y de Seguridad de la Información

Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales, Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto. En la tabla 3. se establecen los criterios para definir el nivel de impacto.

Tabla 3. 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 11 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 51 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 101 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 501 SMLMV.	El riesgo afecta la imagen de la entidad a nivel nacional con efecto publicitario sostenido a nivel país.

Fuente: Adaptado de DAFF, 2020. Guía para la Administración del Riesgo y diseño de controles en entidades públicas.

Tabla 4. Criterios para calificar el impacto – Riesgos de Corrupción

N°	Pregunta Si el riesgo se materializa podría...	Respuesta	
		SI	No
1	¿Afectar al grupo de funcionario del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de la misión de la entidad?		
4	¿Afectar el cumplimiento de la misión del sector a 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 de bien, servicios o recursos públicos?		
9	¿Generar pérdida de la información de la entidad?		
10	¿Generar intervención de los órganos de control, de la fiscalía u otro ente?		
11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		
14	¿Dar lugar a procesos penales?		
15	¿Generar pérdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		

Total de respuestas afirmativas	
Responder afirmativamente de una (1) a cinco (5) preguntas genera un impacto moderado. Responder afirmativamente de seis (6) a once (11) preguntas genera un impacto mayor. Responder afirmativamente de doce (12) a diecinueve (19) preguntas genera un impacto catastrófico.	
MODERADO	Genera medianas consecuencias sobre la entidad
MAYOR	Genera altas consecuencias sobre la entidad
CATASTROFICO	Genera consecuencias desastrosas para la entidad

Fuente: DAFP, 2020, Guía para la Administración de Riesgos y diseño de controles en entidades públicas, V5.

Si la respuesta a la pregunta 16 es afirmativa, el riesgo se considera catastrófico. Por cada riesgo de corrupción identificado, se debe diligenciar una tabla de estas.

iv. Medidas de Tratamiento de Riesgo

El objetivo de esta etapa es identificar las opciones para tratar los riesgos de acuerdo con el nivel de riesgo residual obtenido, esto para procesos en funcionamiento, pero cuando se trate de procesos nuevos se procede a partir del riesgo inherente.

En la empresa se ha definido que los riesgos que se tratan de forma adicional al uso de controles (criterio de aceptabilidad del riesgo), son aquellos que estén en las siguientes situaciones:

✓ Si el riesgo residual es extremo, alto o moderado.
✓ Si hay causas sin controles asociados.
✓ Si hay controles sin evidencias.

Dentro de las actividades a desarrollar en esta etapa se encuentra la de identificar y formalizar las opciones de tratamiento adecuadas, dentro de las cuales se encuentran:

a) **Evitar:** Después de realizar un análisis y considerar que el nivel del riesgo es demasiado alto, se determina NO asumir la actividad que genera este riesgo.

b) **Aceptar:** Después de realizar un análisis y considerar los niveles de riesgo se determina asumir el mismo conociendo los efectos de su posible materialización. Para esta opción se debe tener en cuenta las siguientes consideraciones:

   ✓ En este caso no se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo.

   ✓ La aceptación del riesgo puede ocurrir sin tratamiento, lo que implica que los riesgos aceptados están sujetos a monitoreo.

   ✓Los riesgos de corrupción están excluidos de esta medida de manejo o control. Es decir, ningún riesgo de corrupción podrá ser aceptado.
   ✓ Para el caso de riesgos residuales que sean aceptados por el líder del proceso o dueño del riesgo y que tengan calificación extrema, alta o

moderada, deberá reportarse a la Oficina Asesora de Planeación formalmente a través de un memorando que justifique el porqué de la situación y posteriormente al Comité Institucional de Coordinación de Control Interno.

c) Reducir: Después de realizar un análisis y considerar que el nivel de riesgo es alto, se determina tratarlo mediante mitigar o compartir el riesgo.

✓ **Compartir:** Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, transfiriendo o compartiendo una parte del riesgo. Para el caso que se decida tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas, la responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputacional. De igual forma, los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad.

✓ **Mitigar:** Después de realizar un análisis y considerar los niveles de riesgo se implementan acciones que mitiguen el nivel de riesgo. Por lo tanto, se adoptan medidas para reducir la probabilidad o el impacto del riesgo. No necesariamente es un control adicional.

Nota: Frente al plan de acción referido para la opción de reducir, es importante mencionar que, conceptualmente y de manera general, se trata de una herramienta de planificación empleada para la gestión y control de tareas o proyectos. Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de un plan de acción que especifique: i) responsable, ii) fecha de implementación, y iii) fecha de seguimiento.
Con el propósito de ilustrar las estrategias para combatir los riesgos de gestión y seguridad de la información, en la siguiente tabla se indican las opciones de tratamiento aplicables de acuerdo con la zona de riesgo:

Tabla 5. Opciones de tratamiento Riesgo de Gestión y Seguridad de la Información

Zona de riesgo	Semáforo	Evitar	Reducir		Aceptar
			Compartir	Mitigar	
Extremo	Rojo	X	X	X	X
Alto	Naranja	X	X	X	X
Moderado	Amarillo	X	X	X	X
Bajo	Verde				X

Fuente: Construcción propia 2021

De la misma forma, se ilustran las estrategias para combatir el riesgo de corrupción de acuerdo con la zona de riesgo:

Tabla 6. Opciones de tratamiento Riesgo de Corrupción

Zona de riesgo	Semáforo	Evitar	Reducir		Aceptar
			Compartir	Mitigar	
Extremo	Rojo	X	X	X	
Alto	Naranja	X	X	X	Ningún riesgo de corrupción podrá ser aceptado.
Moderado	Amarillo	X	X	X	
Bajo	Verde				

Fuente: Construcción propia 2021

Nota 1: Para los riesgos de corrupción, la respuesta será evitar, compartir o mitigar el riesgo.
Nota 2: Cuando un riesgo de corrupción se encuentre en zona de riesgo **(Moderado: 3, Rara Vez:1)**, no aplicarán las opciones de tratamiento compartir o reducir el riesgo, ya que en este caso el riesgo se encontrará en su máxima disminución posible dentro del mapa de calor.

v. Periodicidad para el monitoreo, revisión y seguimiento de los riesgos

El monitoreo y revisión de los riesgos corresponde a la Primera Línea de Defensa como un seguimiento constante a la gestión del riesgo y a la efectividad de los controles establecidos. Por otra parte, el monitoreo y revisión realizado por la Oficina de Planeación se lleva a cabo en los siguientes cortes:

- Primer monitoreo: Con corte al 30 de abril. En esa medida, el reporte deberá surtirse dentro de los cinco (05) primeros días del mes de mayo.

- Segundo monitoreo: Con corte al 31 de agosto. El reporte deberá surtirse dentro de los cinco (05) primeros días del mes de septiembre.

- Tercer monitoreo: Con corte al 31 de diciembre. El reporte deberá surtirse dentro de los cinco (05) primeros días del mes de enero.

El Jefe de Control Interno o quien haga sus veces, debe proporcionar un aseguramiento basado en el más alto nivel de independencia y objetividad sobre la efectividad del Sistema de Control Interno. En este sentido es necesario que adelante seguimiento a la gestión del riesgo, verificando la efectividad de los controles. Por consiguiente, de acuerdo con la normatividad, se deberá realizar tres seguimientos a los riesgos corrupción, de acuerdo con lo siguiente:

- Primer seguimiento: Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días del mes de mayo.

- Segundo seguimiento: Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de septiembre.

- Tercer seguimiento: Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de enero.

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

En especial deberá adelantar las siguientes actividades:

- Verificar la publicación del Mapa de Riesgos de Corrupción en la página web de la entidad.

- Seguimiento a la gestión del riesgo.

- Revisión de los riesgos y su evolución.

- Asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma adecuada.

vi. Líneas de Responsabilidad frente a la gestión del riesgo.

Las responsabilidades se definen mediante la línea estratégica y las tres líneas de defensa las cuales se encuentran definidas en la siguiente tabla:

Tabla 7. Responsabilidades

Lineas de Defensa	Responsables	Operatividad
Linea estrategica	Alta Dirección y Comite Institucional de Coordinacion de Control Interno.	Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento Analiza los riesgos y amenazas institucionales al cumplimiento de los planes estrategicos

Lineas de Defensa	Responsables	Operatividad
1ª. Linea de Defensa	Líderes de proceso, programas y proyectos y sus equipos (En general servidores públicos de todos los niveles de la organización).	Desarrollar e implementar procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora, reportando a la segunda línea sus avances o dificultades. Diseñar, implementar y monitorear los controles y gestionar de manera directa en el día a día los riesgos de la entidad. Asimismo, orientar el desarrollo e implementación de políticas y procedimientos internos y asegurar que sean compatibles con las metas y objetivos de la entidad, emprender las acciones de mejoramiento para su logro.
2ª. Linea de Defensa	A cargo de los servidores que tienen responsabilidades directas de monitoreo y revisión de los controles de la gestión de riesgo. Jefes de planeación, supervisores o interventores de proyectos, coordinadores de otros sistemas de gestión de la entidad, coordinadores de equipos de trabajo, comités de riesgos (donde existan), comité de contratación, áreas financieras, Oficina de Información Pública del Interior - OIP, entre otros que generen información para el Aseguramiento de la operación.	Monitorear la gestión de riesgos y control ejecutada por la primera línea de defensa complementando su trabajo. Asegurar que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente, supervisen la implementación de prácticas eficaces de gestión de riesgo. Consolidar y analizar información sobre temas clave para la entidad, base para la toma de decisiones y de las acciones preventivas necesarias para evitar materializaciones de riesgos. Asesorar a la 1ª línea de defensa en temas clave para el Sistema de Control Interno: i) riesgos y controles, ii) planes de mejoramiento, iii) indicadores de gestión, iv) procesos y procedimientos.
3ª. Linea de Defensa	A cargo de la Oficina de Control Interno, Auditoría Interna o quien haga sus veces.	Proporcionar un aseguramiento basado en el más alto nivel de independencia y objetividad sobre la efectividad del Sistema de Control Interno. El alcance de este aseguramiento, a través de la auditoría interna, cubre todos los componentes del Sistema de Control Interno. Genera a través de su rol de asesoría una orientación técnica y recomendaciones frente a la administración del riesgo en coordinación con la Oficina Asesora de Planeación o quien haga sus veces. Monitorear la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo. Brinda un nivel de asesoría proactiva y estratégica frente a la Alta Dirección y los líderes de proceso.

vii. Comunicación

Esta estrategia de comunicación busca socializar e interiorizar en todos los servidores públicos y terceros que presten sus servicios al Ministerio del Interior, de los distintos niveles de responsabilidad, sobre la importancia de la gestión del riesgo así:

• **Nivel institucional:** La Oficina de Planeación liderará las acciones tendientes a la consolidación, socialización y comunicación de la gestión de riesgos en la Empresa; este consolidado atenderá a las necesidades de información de los grupos interesados y se publicará en la página web de la Entidad de acuerdo con lo programado en el Plan Anticorrupción y Atención al Ciudadano. Así mismo, de acuerdo con los niveles de responsabilidad establecidos en las líneas de defensa, el monitoreo y revisión por parte de la primera y segunda línea de defensa y, seguimiento por parte de la tercera línea de defensa.

• **Nivel de procesos:** Teniendo en cuenta las responsabilidades sobre una base del día a día estará a cargo de los líderes de proceso y consiste en realizar la divulgación de los mapas de riesgos por proceso al interior de sus respectivos equipos de trabajo.

MARTHA PATRICIA CORREA T.
Gerente.

15 JUN 2022

Actualizó y proyectó: Mauricio García escobar, jefe de Control Interno.
Revisó: Diego Ocazionez, Secretario general.