POLITICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL

Establecimiento Público Ambiental del Distrito de Buenaventura EPA

Director
Carlos Javier Cruz
Subdirector de Planeación
José Ignacio Girón Ortiz
Subdirector Administrativo y Financiero
Héctor Fabio Aguilar

Sabina Collazos R

Tabla de contenido

1 MARCO NORMATIVO 2

2 TERMINOS Y DEFINICIONES 2

3 POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL DE EPA 5

3.1 Objetivo de la política 5

3.2 Alcance de la Política 6

3.3 Niveles de aceptación del riesgo o tolerancia al riesgo 6

3.4 Establecimiento de la Política 6

3.5 Niveles de aceptación del riesgo 6

3.6 Niveles para calificar el impacto 7

3.7 Tratamiento de Riesgos 8

4 IDENTIFICACION DE RIESGOS 8

4.1 Establecimiento del contexto 8

4.1.1 Establecimiento del contexto externo 8

4.1.2 Establecimiento del contexto interno 8

4.1.3 Establecimiento del contexto por proceso 8

4.1.4 Identificación de activos de seguridad de la información 10

5 VALORACION DE RIESGOS 13

5.1 Análisis de Riesgos 14

5.1.1 Análisis de causas 14

5.1.2 Determinar la probabilidad 14

5.1.3 Determinar consecuencias o nivel de impacto 15

5.2 Evaluación de Riesgos 20

5.2.1 Análisis preliminar (riesgo inherente) 20

5.2.2 Valoración de los controles –diseño de controles 21

5.2.3 Nivel de riesgo (residual) 22

5.3 Monitoreo y Revisión. 23

5.4 Seguimiento riesgos de corrupción 27

1 MARCO NORMATIVO

Ley 87 de 1993: Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones. (Modificada parcialmente por la Ley 1474 de 2011). Artículo2 Objetivos del Control Interno: Literal a).Proteger los recursos de la organización, buscando adecuada administración ante posibles riesgos que los afectan. Literal f). Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos.

Ley 1474 de 2011: Estatuto Anticorrupción Artículo73. "Plan Anticorrupción y de Atención al Ciudadano" que deben elaborar anualmente todas las entidades, incluyendo el mapa de riesgos de corrupción, las medidas concretas para mitigar esos riesgos, las estrategias anti-trámites y los mecanismos para mejorar la atención al ciudadano

Decreto 943 del 21 de mayo de 2014: Por el cual se actualiza el Modelo Estándar de Control Interno (MECI).

Guía para la administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el diseño de controles en entidades públicas.- Departamento Administrativo de la Función Pública.

ISO 31000:2009 Norma Técnica Internacional Gestión del Riesgo- Principios y directrices

2 TERMINOS Y DEFINICIONES

- **Causas**: Son los medios, circunstancias y agentes generadores del riesgo.
- **Compartir el Riesgo**: Reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, procesos, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Es así como por ejemplo, la información de gran importancia se puede duplicar

y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar.

- **Consecuencias**: El resultado real o potencial sea este una pérdida, perjuicio, desventaja o ganancia, frente a la consecución de los objetivos del proceso o de la entidad.
- **Contexto Externo**: Ambiente externo en el cual la organización busca alcanzar sus objetivos que puede ser: ambiente cultural, social, político, legal, reglamentario, financiero, tecnológico, económico, natural y competitivo, nacional, regional o local.
- **Contexto Interno**: Ambiente interno en el cual la organización busca alcanzar sus objetivos, el cual puede ser: gobierno, estructura organizacional, funciones, responsabilidades, políticas, normas, directrices adoptadas por la organización, objetivos, estrategias implementadas, recursos (capital, tiempo, personas, procesos, sistemas, tecnologías).
- **Contexto Estratégico**: Insumo básico para la identificación de los riesgos en los procesos y actividades, el análisis se realiza a partir del conocimiento de situaciones internas y externas de la institución.
- **Control:** Acciones establecidas para disminuir la probabilidad de ocurrencia del riesgo, el impacto de los riesgos y/o asegurar la continuidad del servicio en caso de llegarse a materializar el riesgo.
- **Controles Correctivos**: Aquellos que permiten el restablecimiento de la actividad después de ser detectado un evento no deseable; también permiten la modificación de las acciones que propiciaron su ocurrencia.
- **Controles Preventivos:** Aquellos que actúan para eliminar las causas del riesgo, para prevenir su ocurrencia o materialización.
- **Evaluación del Riesgo**: Proceso utilizado para determinar las prioridades de la administración del riesgo, comparando el nivel de un determinado riesgo con respecto a un estándar determinado.
- **Evento**: Incidente o situación potencial que puede ocurrir en un lugar determinado durante un periodo determinado. Este puede ser cierto o incierto y su ocurrencia puede ser única o ser parte de una serie de causas.

- **Evitar el Riesgo**: Tomar las medidas encaminadas a prevenir su materialización. Es siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se genera cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas.

- **Frecuencia**: Medida del coeficiente de ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.

- **Gestión del Riesgo**: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo y proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

- **Impacto:** Consecuencias que puede ocasionar a la entidad la materialización del riesgo.

- **Mapa de Riesgos**: Herramienta metodológica que permite hacer un inventario de los riesgos ordenada y sistemáticamente, definiéndolos, haciendo la descripción de cada uno de estos y las posibles consecuencias y sus acciones preventivas.

- **Monitorear**: Comprobar, supervisar, observar o registrar la forma en que se lleva a cabo una actividad con el fin de identificar posibles cambios.

- **Plan de Manejo del Riesgo**: Parte del plan de manejo de riesgos que contiene las acciones a ejecutar en caso de la materialización del riesgo, con el fin de dar continuidad a los objetivos de la entidad.

- **Política de Riesgos**: Intención global u orientación de una entidad frente a la gestión del riesgo.

- **Probabilidad:** Grado en el cual es probable que ocurra un evento, que se debe medir a través de la relación entre los hechos ocurridos realmente y la cantidad de eventos que pudieron ocurrir.

- **Riesgo de Corrupción**: La posibilidad de que por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular.

- **Riesgo Inherente**: es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.
- **Riesgo Residual**: nivel de riesgo que permanece luego de tomar medidas de tratamiento de riesgo.
- **Riesgo:** Es el resultado de la combinación entre la probabilidad de ocurrencia de un evento y sus posibles consecuencias que tendrán un impacto mayor o menor sobre la capacidad de lograr los objetivos.
- **Valoración del Riesgo:** Elemento de Control, que determina el nivel o grado de exposición de la entidad pública al impacto del riesgo, permitiendo estimar las prioridades para su tratamiento según El Decreto 1599 de 2005.

3 POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL DE EPA

EPA –Establecimiento Público Ambiental –Distrito de Buenaventura define su política del riesgo atendiendo los lineamientos establecidos en la Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas DAFP[1], articulada con las normas aplicables a la Entidad y al sistema de gestión de la calidad, se compromete a identificar, analizar, valorar, monitorear, administrar y tratar los riesgos que pudieran afectar el logro de los objetivos estratégicos y los procesos de la entidad.

3.1 Objetivo de la política

[1]Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas. Agosto de 2018.

Establecer los principios básicos y el marco general de actuación para el control y la gestión de los riesgos de toda naturaleza a los que se enfrenta la entidad así como:

- ✓ Suministrar una metodología que permita a EPA gestionar de manera efectiva los riesgos que afectan el logro de los objetivos estratégicos y de proceso.

- ✓ Ofrecer herramientas para identificar, analizar, evaluar los riesgos y determinar roles y responsabilidades de cada uno de los servidores de la entidad (Esquema de las Líneas de Defensa) en los riesgos de gestión y en los riesgos de corrupción el monitoreo y seguimiento.

- ✓ Suministrar lineamientos basados en una adecuada gestión del riesgo y control a los mismos, que permitan a la alta dirección de las entidades tener una seguridad razonable en el logro de sus objetivos.

3.2 Alcance de la Política

Aplica para la gestión de riesgos de todos los procesos de EPA proyectos y a todas las acciones ejecutadas por los servidores durante el ejercicio de sus funciones. Incluye los riesgos de gestión, corrupción y seguridad digital.

3.3 Niveles de aceptación del riesgo o tolerancia al riesgo

Establece “los niveles aceptables de desviación relativa a la consecución de los objetivos” (NTC GTC 137 Numeral 3.7.16), los mismos están asociados a la estrategia de la entidad y pueden considerarse para cada uno de los procesos. Los riesgos de corrupción son inaceptables.

3.4 Establecimiento de la Política

Es responsabilidad de La Alta Dirección de EPA con el liderazgo del representante legal y la participación del Comité Institucional de Coordinación de Control Interno.

3.5 Niveles de aceptación del riesgo

Decisión informada de tomar un riesgo particular. (NTC GTC137, al riesgo: Numeral 3.7.1.6) Para riesgo de corrupción es inaceptable.

3.6 Niveles para calificar el impacto

Esta tabla de análisis variará de acuerdo con la complejidad de cada entidad, será necesario considerar el sector al que pertenece (riesgo de la operación, los recursos humanos y físicos con los que cuenta, su capacidad financiera, usuarios a los que atiende, entre otros aspectos).

Nivel	Impacto (consecuencias) Cuantitativo	Impacto (consecuencias) Cualitativo
CATASTRÓFICO	- Impacto que afecte la ejecución presupuestal en un valor ≥50% - Pérdida de cobertura en la prestación de los servicios de la entidad ≥50%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥50% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de laentidad.	- Interrupción de las operaciones de la Entidad por más de cinco (5) días. - Intervención por parte de un ente de control u otro ente regulador. - Pérdida de Información crítica para la entidad que no se puederecuperar. - Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. - Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.
MAYOR	- Impacto que afecte la ejecución presupuestal en un valor ≥20% - Pérdida de cobertura en la prestación de los servicios de la entidad ≥20%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥20% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥20% del presupuesto general de la entidad.	- Interrupción de las operacionesde la Entidad por más de dos (2) días. - Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. - Sanción por parte del ente de control u otro ente regulador. - Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. - Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.
MODERADO	- Impacto que afecte la ejecución presupuestal en un valor ≥5% - Pérdida de cobertura en la prestación de los servicios de la entidad ≥10%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥5% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥5% del presupuesto general de laentidad.	- Interrupción de las operaciones de la Entidad por un (1) día. - Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. - Inoportunidad en la información ocasionando retrasos en la atención a los usuarios. - Reproceso de actividades y aumento de carga operativa. - Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. - Investigaciones penales, fiscales o disciplinarias.
MENOR	- Impacto que afecte la ejecución presupuestal en un valor ≥1% - Pérdida de cobertura en la prestación de los servicios de la entidad ≥5%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥1% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥1%del presupuestogeneral de la entidad.	- Interrupción de las operaciones de la Entidad por algunas horas. - Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias. - Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.
INSIGNIFICANTE	- Impacto que afecte la ejecución presupuestal en un valor ≥0,5% - Pérdida de cobertura en la prestación de los servicios de la entidad ≥1%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥0,5% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥0,5%del presupuesto general de la entidad.	- No hay interrupción de las operaciones de la entidad. - No se generan sanciones económicas o administrativas. - No se afecta la imagen institucional de forma significativa.

3.7 Tratamiento de Riesgos

Proceso para modificar el riesgo (NTC GTC137, Numeral 3.8.1)

4 IDENTIFICACION DE RIESGOS

4.1 Establecimiento del contexto

Define los parámetros internos y externos que se han de tomar en consideración para la administración del riesgo (NTCISO 31000). A partir de la definición de estos, es posible establecer las causas de los riesgos a identificar.

4.1.1 Establecimiento del contexto externo

Está determinado por las características o aspectos esenciales del entorno en el cual opera la entidad. Se consideran factores como:

- ✓ Económicos
- ✓ Políticos
- ✓ Sociales
- ✓ Tecnológicos
- ✓ Medioambientales
- ✓ Comunicación externa

4.1.2 Establecimiento del contexto interno

Está determinado por las características o aspectos esenciales del ambiente en el cual la organización busca alcanzar sus objetivos. Se consideran factores como:

- ✓ Financieros
- ✓ Personal
- ✓ Procesos
- ✓ Tecnología
- ✓ Estratégicos
- ✓ Comunicación Interna

4.1.3 Establecimiento del contexto por proceso

Está determinado por las características o aspectos esenciales del proceso y sus interrelaciones. Se consideran factores como:

- ✓ Diseño del proceso
- ✓ Interacciones con otros procesos
- ✓ Transversalidad
- ✓ Procedimientos asociados
- ✓ Responsables del procesos
- ✓ Comunicación entre los procesos
- ✓ Archivos de seguridad digital del proceso.

	FACTORES PARA CADA CATEGORIA DEL PROCESO
CONTEXTO EXTERNO	**ECONÓMICOS**: disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia
	POLÍTICOS: cambios de gobierno, legislación, políticas públicas, regulación.
	SOCIALES: demografía, responsabilidad social, orden público.
	TECNOLÓGICOS: avances en tecnología, acceso a sistemas de información externos, gobierno en línea
	MEDIOAMBIENTALES: emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.
	COMUNICACIÓN EXTERNA:mecanismos utilizados para entrar en contacto con los usuarios o ciudadanos, canales establecidos para que el mismo se comunique con la entidad.
CONTEXTO INTERNO	**FINANCIEROS:** presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.
	PERSONAL: competencia del personal, disponibilidad del personal, seguridad y salud ocupacional.
	PROCESOS: capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.
	TECNOLOGÍA: integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información.
	ESTRATÉGICOS: direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo.
	COMUNICACIÓN INTERNA: canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.
CONTEXTO DEL PROCESO	**DISEÑO DEL PROCESO:** claridad en la descripción del alcance y objetivo del proceso.
	INTERACCIONES CON OTROS PROCESOS: relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.
	TRANSVERSALIDAD: procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.
	PROCEDIMIENTOS ASOCIADOS: pertinencia en los procedimientos que desarrollan los procesos.
	RESPONSABLES DEL PROCESO: grado de autoridad y responsabilidad de los funcionarios frente al proceso.
	COMUNICACIÓN ENTRE LOS PROCESOS: efectividad en los flujos de información determinados en la interacción de los procesos.
	ACTIVOS DE SEGURIDAD DIGITAL DEL PROCESO: información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso, como de cara al ciudadano. Ver conceptos básicos relacionados con el riesgo páginas 10 y 11.

4.1.4 Identificación de activos de seguridad de la información

- **Identificación de activos:** Le corresponde a la primera línea de defensa, realizar la identificación de activos en cada proceso.

- **Un activo es** cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital son activos elementos tales como (aplicaciones de la organización, servicios web, redes, información física o digital, tecnologías de información -TI-, tecnologías de operación -TO-) que utiliza la organización para funcionar en el entorno digital.

- **Los activos se deben identificar** pues de esta manera se puede determinar qué es lo más importante que cada entidad y sus procesos poseen (sean bases de datos, unos archivos, servidores web o aplicaciones claves para que la entidad pueda prestar sus servicios). Así la entidad puede saber qué es lo que debe proteger para garantizar tanto su funcionamiento tanto interno como su funcionamiento de cara al ciudadano, aumentando así su confianza en el uso del entorno digital.

-

¿Cómo identificar los activos?

4.2 Identificación de riesgos

La identificación del riesgo se realiza determinando las causas con base en el contexto interno, externo y del proceso que pueden afectar el logro de los objetivos.

Algunas causas externas no controlables por la entidad se podrán evidenciar en el análisis del contexto externo, para ser tenidas en cuenta en el análisis y valoración del riesgo.

A partir de este contexto se identifica el riesgo, el cual estará asociado a aquellos eventos o situaciones que pueden entorpecer el normal desarrollo de los objetivos del Proceso o estratégicos. Las preguntas claves para la identificación del riesgo permiten determinar:

¿QUÉ PUEDE SUCEDER? *Identificar la afectación del cumplimiento del objetivo estratégico o del proceso según sea el caso.*

¿CÓMO PUEDE SUCEDER? *Establecer las causas a partir de los factores determinados en el contexto*

¿CUÁNDO PUEDE SUCEDER? *Determinar de acuerdo al desarrollo del proceso*

¿QUÉ CONSECUENCIAS TENDRÍA SU MATERIALIZACIÓN? *Determinar los posibles efectos por la materialización del riesgo*

Definición de 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.

"Esto implica que las prácticas corruptas son realizadas por actores públicos y/o privados con poder e incidencia en la toma de decisiones y la administración de los bienes públicos". (Conpes N° 167 de 2013).

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

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

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

Los riesgos de corrupción se establecen sobre **procesos.**

El riesgo debe estar descrito de manera clara y precisa. Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos.

Con el fin de facilitar la identificación de riesgos de corrupción y evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción, se sugiere la utilización de la **matriz de definición de riesgo de corrupción**, que incorpora cada uno de los componentes de su definición. Si en la descripción del riesgo, las casillas son contestadas todas afirmativamente, se trata de un riesgo de corrupción, así:

Matriz definición del riesgo de corrupción				
Descripción del riesgo	Acción u omisión	Uso del poder	Desviar la gestión de lo público	Beneficio privado
Posibilidad de recibir o solicitar cualquier dadiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato	X	X	X	X

Generalidades riesgos de corrupción

Entidades encargadas de gestionar el riesgo: lo deben adelantar las entidades del orden nacional, departamental y municipal.

• Se elabora anualmente por cada responsable de los procesos al interior de las entidades, junto con su equipo.

• **Consolidación**: la oficina de planeación o quien haga sus veces, o a la de dependencia encargada de gestionar el riesgo le corresponde liderar el proceso de administración de estos. Adicionalmente, esta misma oficina será la encargada de consolidar el mapa de riesgos de corrupción.

• **Publicación del mapa de riesgos de corrupción:** se debe publicar en la página web de la entidad, en la sección particular de transparencia y acceso a la información pública que establece el artículo 2.1.1.2.1.4 del Decreto 1081 de 2015 o en medio de fácil acceso al ciudadano, a más tardar el 31 de enero de cada año.

La publicación será parcial, y fundamentada en la elaboración del Índice de Información Clasificada y Reservada. En dicho instrumento la entidad debe establecer las condiciones de reserva y clasificación de algunos de los elementos constitutivos del mapa de riesgos en los términos dados en los artículos 18 y 19 de la Ley 1712 de 2014)

En este caso, se deberá anonimizar esa información. Es decir, la parte clasificada o reservada, aunque se elabora no se hace visible en la publicación.

Recuerde que las excepciones solo pueden estar establecidas en una la ley, un decreto con fuerza de ley, o un tratado internacional ratificado por el Congreso o en la Constitución.

• **Socialización**: Los servidores públicos y contratistas de la entidad deben conocer su contenido antes de su publicación. Para lograr este propósito la oficina de planeación o quien haga sus veces o la de gestión del riesgo, deberá diseñar y poner en marcha las actividades o mecanismos necesarios para que los funcionarios y contratistas conozcan, debatan y formulen sus apreciaciones y propuestas sobre el proyecto del Mapa de Riesgos de Corrupción.

Así mismo, dicha oficina adelantará las acciones para que la ciudadanía y los interesados externos conozcan y manifiesten sus consideraciones y sugerencias sobre el proyecto del mapa de riesgos de corrupción. Deberá dejarse la evidencia del proceso de socialización y publicarse sus resultados.

• **Ajustes y modificaciones**: después de su publicación y durante el respectivo año de vigencia, se podrán realizar los ajustes y las modificaciones necesarias orientadas a mejorar el Mapa de Riesgos de Corrupción. En este caso deberá dejarse por escrito los ajustes, modificaciones o inclusiones realizadas.

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

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

TIPOLOGIA DE RIESGOS	**Riesgos estratégicos**: posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública y por tanto impactan toda la entidad.
	Riesgos gerenciales: posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la alta dirección.
	Riesgos operativos: posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad.
	Riesgos financieros: posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, central de cuentas, costos, etc.
	Riesgos tecnológicos: posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.
	Riesgos de cumplimiento: posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones contractuales.
	Riesgo de imagen o reputacional: posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización, ante sus clientes y partes interesadas.
	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.
	Riesgos de seguridad digital: Posibilidad Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

5 VALORACION DE RIESGOS

Consiste en establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial. (RIESGO INHERENTE)

5.1 Análisis de Riesgos

Se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE).

5.1.1 Análisis de causas

Los objetivos estratégicos y de proceso se desarrollan a través de actividades, pero no todas tienen la misma importancia, por tanto se debe establecer cuáles de ellas contribuyen mayormente al logro de los objetivos y estas son las actividades críticas o factores claves de éxito; estos factores se deben tener en cuenta al identificar las causas que originan la materialización de los riesgos.

5.1.2 Determinar la probabilidad

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.

Por PROBABILIDAD se entiende la posibilidad de ocurrencia del riesgo, ésta puede ser medida con criterios de Frecuencia o Factibilidad.

Bajo el criterio de FRECUENCIA se analizan el # 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

Bajo el criterio de FACTIBILIDAD se analiza 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 se dé.

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.

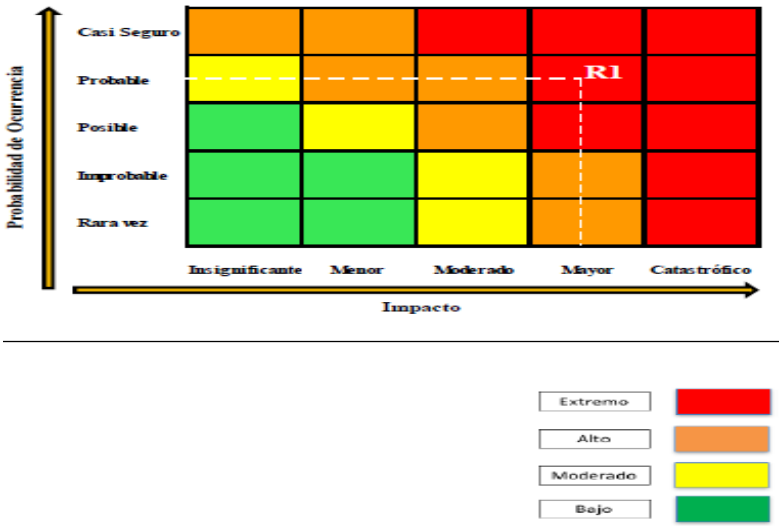
5.1.3 Determinar consecuencias o nivel de impacto

El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo.

Para el ejemplo que venimos explicando, el impacto fue identificado como **mayor** por cuanto genera interrupción de las operaciones por más de dos días.

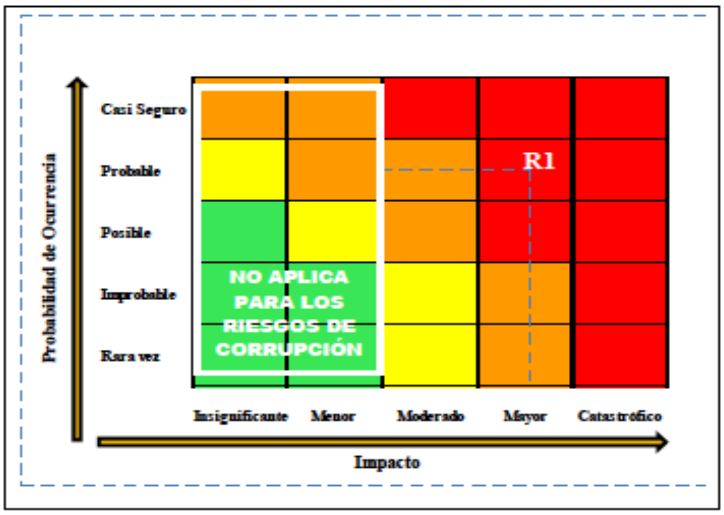
MAPA DE CALOR
Se toma la calificación de probabilidad (resultante de la tabla Matriz de priorización de probabilidad), en el ejemplo: **probable** y la calificación de impacto, para nuestro ejemplo: **mayor;** ubique la calificación de probabilidad en la fila y la de impacto en la columnas correspondientes, establezca el punto de intercepción de las dos y este punto corresponderá al nivel de riesgo, que para el ejemplo es nivel extremo – color rojo (**R1**) determinando así el riesgo inherente.

Mapa de calor (riesgo inherente)



Nivel	Impacto (consecuencias) Cuantitativo	Impacto (consecuencias) Cualitativo
CATASTRÓFICO	- Impacto que afecte la ejecución presupuestal en un valor ≥50% - Pérdida de cobertura en la prestación de los servicios de la entidad ≥50%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥50% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de laentidad.	- Interrupción de las operaciones de la Entidad por más de cinco (5) días. - Intervención por parte de un ente de control u otro ente regulador. - Pérdida de Información crítica para la entidad que no se puederecuperar. - Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. - Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.
MAYOR	- Impacto que afecte la ejecución presupuestal en un valor ≥20% - Pérdida de cobertura en la prestación de los servicios de la entidad ≥20%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥20% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥20% del presupuesto general de la entidad.	- Interrupción de las operacionesde la Entidad por más de dos (2) días. - Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. - Sanción por parte del ente de control u otro ente regulador. - Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. - Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.
MODERADO	- Impacto que afecte la ejecución presupuestal en un valor ≥5% - Pérdida de cobertura en la prestación de los servicios de la entidad ≥10%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥5% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥5% del presupuesto general de laentidad.	- Interrupción de las operaciones de la Entidad por un (1) día. - Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. - Inoportunidad en la información ocasionando retrasos en la atención a los usuarios. - Reproceso de actividades y aumento de carga operativa. - Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. - Investigaciones penales, fiscales o disciplinarias.
MENOR	- Impacto que afecte la ejecución presupuestal en un valor ≥1% - Pérdida de cobertura en la prestación de los servicios de la entidad ≥5%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥1% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥1%del presupuestogeneral de la entidad.	- Interrupción de las operaciones de la Entidad por algunas horas. - Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias. - Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.
INSIGNIFICANTE	- Impacto que afecte la ejecución presupuestal en un valor ≥0,5% - Pérdida de cobertura en la prestación de los servicios de la entidad ≥1%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥0,5% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥0,5%del presupuesto general de la entidad.	- No hay interrupción de las operaciones de la entidad. - No se generan sanciones económicas o administrativas. - No se afecta la imagen institucional de forma significativa.

Mapa de calor (riesgo inherente)

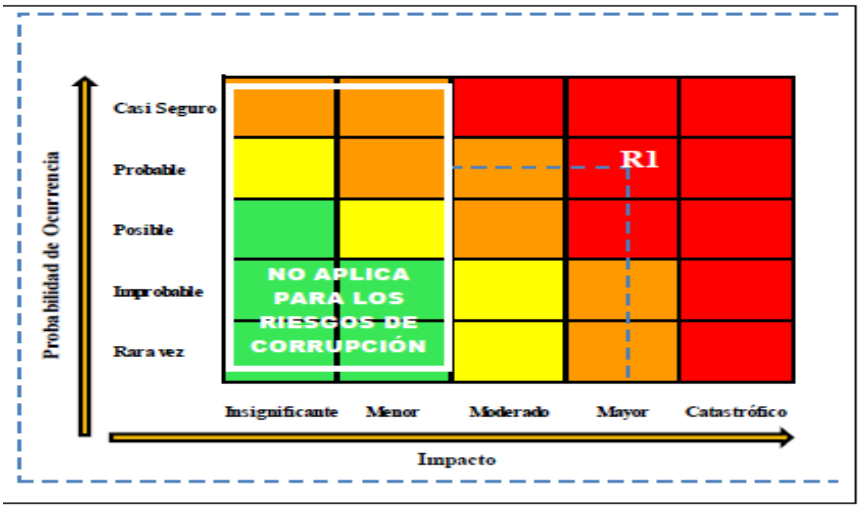


Fuente: Secretaría de Transparencia de la Presidencia de la República

Análisis de impacto en riesgos de corrupción

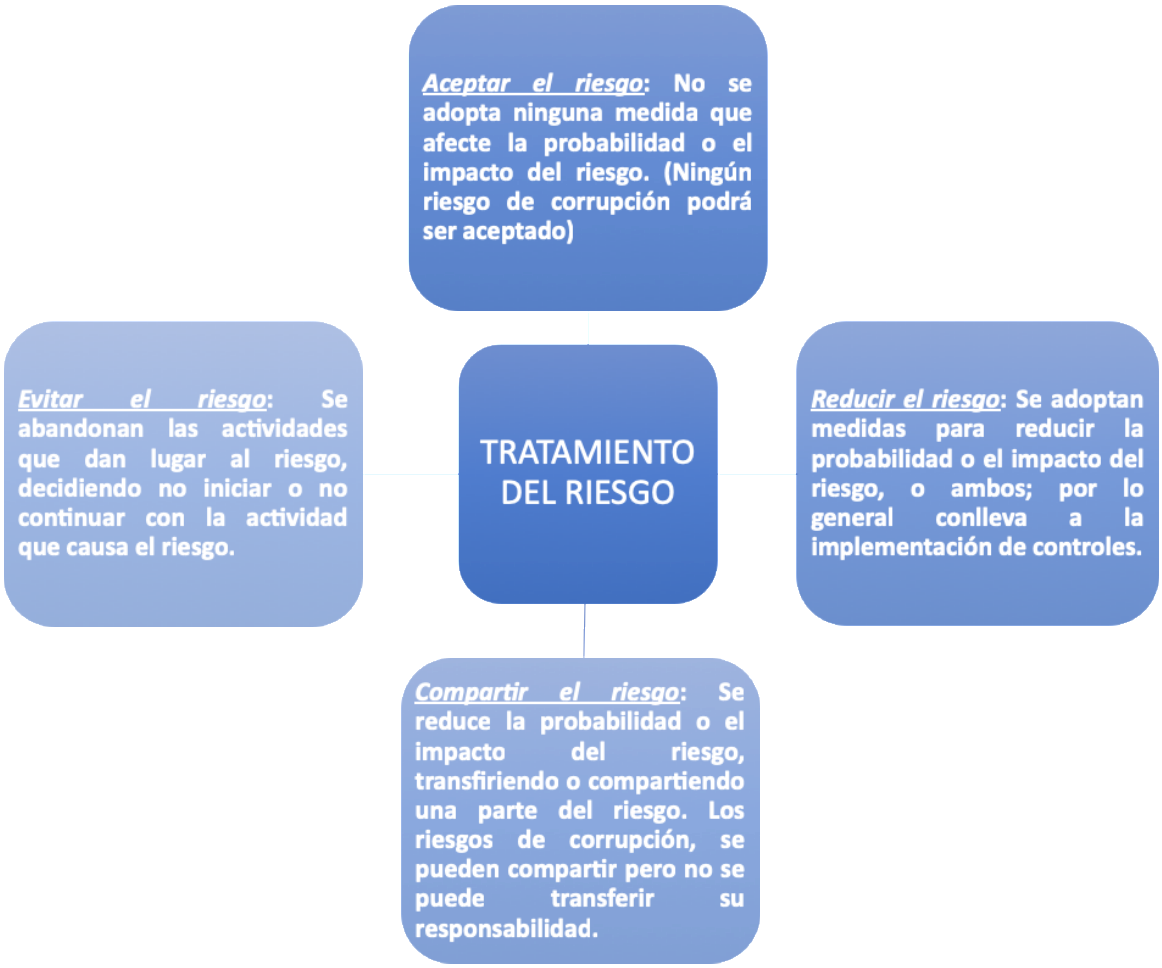
Para los riesgos de corrupción, **el análisis de impacto** se realizará teniendo en cuenta solamente los niveles moderado, mayor y catastrófico, dado que estos riesgos siempre serán significativos; en este orden de ideas, no aplican los niveles de impacto insignificante y menor, que si aplican para los demás riesgos.

Mapa de calor (riesgo inherente)



Tratamiento del Riesgo

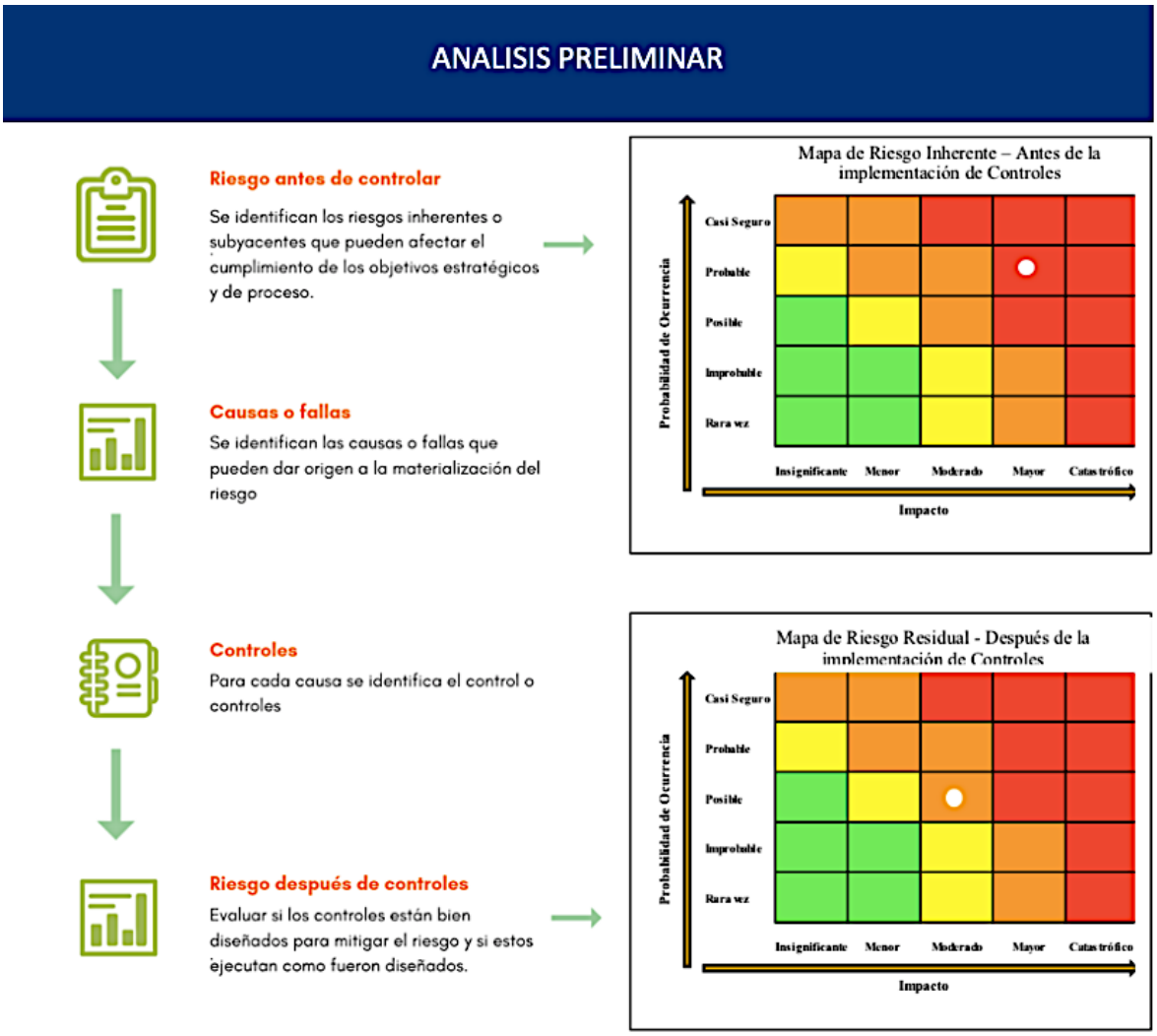
Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo los riesgos de Corrupción. A la hora de evaluar las opciones existentes en materia de tratamiento del riesgo, y partiendo de lo que establezca la política de administración del riesgo, los dueños de los procesos tendrán en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto del riesgo, y la relación costo beneficio de las medidas de tratamiento.
Pero en caso de que una respuesta ante el riesgo, derive en un riesgo residual que supere los niveles aceptables para la dirección, se deberá volver a analizar y revisar dicho tratamiento. En todos los casos para los riesgos de corrupción, la respuesta será evitar, compartir o reducir el riesgo. El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:



5.2 Evaluación de Riesgos

5.2.1 Análisis preliminar (riesgo inherente)

Al momento de definir las actividades de control por parte de la Primera Línea de Defensa, es importante considerar que los controles estén bien diseñados, es decir, que estos mitigan las causas que hacen que el riesgo se materialice.



5.2.2 Valoración de los controles –diseño de controles

Antes de valorar los controles, es necesario conocer cómo se diseña un control, para lo cual daremos respuesta a las siguientes interrogantes:
¿Cómo defino o establezco un control para que en su diseño, mitigue de manera adecuada el riesgo?

Las variables a evaluar para el adecuado diseño de controles son:

PASO 1	**Debe tener definido el responsable de realizar la actividad de control.**
PASO 2	**Debe tener una periodicidad definida para su ejecución.**
PASO 3	**Debe indicar cuál es el propósito del control.**
PASO 4	**Debe establecer el cómo se realiza la actividad de control.**
PASO 5	**Debe indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control.**
PASO 6	**Debe dejar evidencia de la ejecución del control.**

Análisis y evaluación del diseño del control de acuerdo con las seis (6) variables establecidas:

Criterio de evaluación	Aspecto a Evaluar en el Diseño del Control	Opciones de respuesta	
1. Responsable	¿Existe un responsable asignado a la ejecución del control?	Asignado	No asignado
	¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	Adecuado	Inadecuado
2. Periodicidad	¿La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna?	Oportuna	Inoportuna
3. Propósito	¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, ejemplo Verificar, Validar Cotejar, Comparar, Revisar, etc.?	Prevenir o detectar	No es un control
4. Cómo se realiza la actividad de control	¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?.	Confiable	No confiable
5. Qué pasa con las observaciones o desviaciones	¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?	Se investigan y resuelven oportunamente	No se investigan y resuelven oportunamente.
6. Evidencia de la ejecución del control	¿Se deja evidencia o rastro de la ejecución del control, que permita a cualquier tercero con la evidencia, llegar a la misma conclusión?.	Completa	Incompleta / no existe

5.2.3 Nivel de riesgo (residual)

Dado que ningún riesgo con una medida de tratamiento se evita o elimina, el desplazamiento de un riesgo inherente en su probabilidad o impacto para el cálculo del riesgo residual, se realizará de acuerdo a la siguiente tabla:

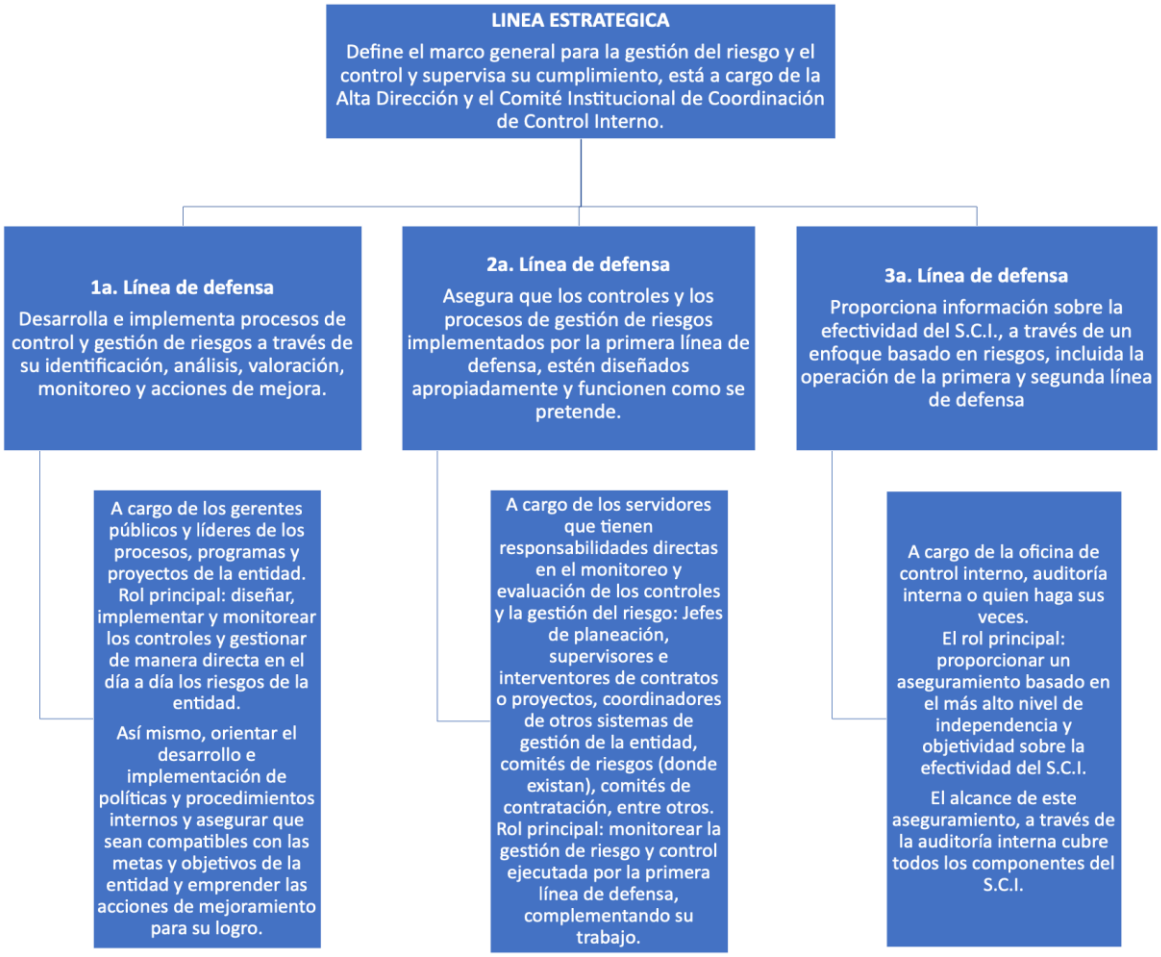
Resultados de los posibles desplazamientos de la probabilidad y del impacto de los riesgos				
Solidez del conjunto de los controles.	Controles ayudan a disminuir la probabilidad	Controles ayudan a disminuir impacto	# Columnas en la matriz de riesgo que se desplaza en el eje de la probabilidad	# Columnas en la matriz de riesgo que se desplaza en el eje de impacto
fuerte	directamente	directamente	2	2
fuerte	directamente	indirectamente	2	1
fuerte	directamente	no disminuye	2	0
fuerte	no disminuye	directamente	0	2
moderado	directamente	directamente	1	1
moderado	directamente	indirectamente	1	0
moderado	directamente	indirectamente	1	0
moderado	no disminuye	directamente	0	1

5.3 Monitoreo y Revisión.

Se debe monitorear y revisar la gestión de riesgos pues la entidad debe asegurar el logro de sus objetivos, anticipándose a los eventos negativos relacionados con la gestión de la Entidad. El Modelo Integrado de Plantación y Gestión- (MIPG) en la dimensión 7 “Control Interno” desarrolla a través de las Líneas de Defensa la responsabilidad de la gestión del riesgo y control.

Las líneas de defensa es un modelo de control que establece los roles y responsabilidades de todos los actores del riesgo y control en una entidad, este proporciona aseguramiento de la gestión y previene la materialización de los riesgos en todos sus ámbitos

El monitoreo y revisión de la gestión de riesgos, está alineado con la dimensión del MIPG de “Control Interno”, que se desarrolla con el MECI a través de un esquema de asignación de responsabilidades y roles, el cual se distribuye en diversos servidores de la Entidad como sigue:



Monitoreo riesgos de corrupción

Los líderes de los procesos en conjunto con sus equipos deben monitorear y revisar
Periódicamente la gestión de riesgos de corrupción y si es del caso ajustarlo, (primera línea de defensa). Le corresponde, igualmente a la oficina de planeación adelantar el monitoreo, (segunda línea de defensa) para este propósito se sugiere elaborar una matriz para el monitoreo periódico. Este monitoreo será en los tiempos que determine la entidad.

Su importancia radica en la necesidad de monitorear permanentemente la gestión del riesgo y la efectividad de los controles establecidos. Teniendo en

cuenta que la corrupción es -por sus propias características una actividad difícil de detectar.

Para el efecto deben atender las actividades descritas en la primera y segunda línea de defensa de este documento.

REPORTE PLAN DE TRATAMIENTO DE DATOS

CONSOLIDAR LA INFORMACIÓN PARA LA GESTIÓN DEL RIESGO

Una vez analizado el nivel de riesgo residual y definido el tratamiento a implementar con el establecimiento de controles preventivos y detectivos, es necesario generar un reporte que consolide la información clave del proceso de gestión del riesgo.

En el formato de Mapa y Plan de Tratamiento de Riesgos, se inicia con el registro del riesgo identificado, luego se especifica la clase de riesgo, se transcriben las causas raíz o causas priorizadas, así como la probabilidad e impacto que quedaron después de valorar los controles para determinar el riesgo residual.

A partir de allí se deben analizar las estrategias DO y FA o estrategias de supervivencia formuladas en la etapa de establecimiento del contexto, que contrarresten las causas raíz, para colocarlas en las actividades de control del formato y con base en su contenido se establezca la opción de tratamiento a la que corresponden.

Luego se relaciona el soporte con el que se evidenciará el cumplimiento de cada actividad, el responsable de adelantarla (relacionando el cargo y no el nombre), el tiempo específico para cumplir con la actividad o la periodicidad de ejecución.

Al final de todas las actividades de control establecidas para atacar las causas del riesgo, se debe relacionar la acción de contingencia a implementar una vez el riesgo se materialice, para ello se deben analizar las estrategias DA o estrategias de fuga provenientes de la Matriz DOFA, seleccionando la(s) más apropiada(s) para el riesgo identificado

No olvidar colocar el soporte, responsable y tiempo de ejecución, teniendo en cuenta que este tipo de acciones son de aplicación inmediata y a corto plazo para restablecer cuanto antes, la normalidad de las actividades para el logro de los objetivos del proceso o la estrategia.

Por último se formulan los indicadores clave de riesgo (KRI por sus siglas en ingles) que permitan monitorear el cumplimiento (eficacia) e impacto (efectividad) de las actividades de control, siempre y cuando conduzcan a la toma de decisiones (Por riesgo identificado en los procesos).

5.4 Seguimiento riesgos de corrupción

El Jefe de Control Interno o quien haga sus veces, debe adelantar seguimiento al Mapa de Riesgos de Corrupción. En este sentido es necesario que adelante seguimiento a la gestión del riesgo, verificando la efectividad de los controles.

- Primer seguimiento: Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro delos 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 lugar de fácil acceso al ciudadano.

En especial deberá adelantar las siguientes actividades:

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

Acciones a seguir en caso de materialización de riesgos de corrupción

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

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

Teniendo en cuenta que la Oficina de Control Interno debe asegurar que los controles sean efectivos, le apunten al riego y están funcionando en forma oportuna y efectiva.

Las acciones adelantadas se refieren a:

- Acciones encaminadas a determinar la efectividad de los controles.
- Acciones encaminadas a mejorar la valoración de los riesgos.
- Acciones encaminadas a mejorar los controles.
- Analizar el diseño e idoneidad de los controles, si son adecuados para prevenir o mitigar los riesgos de corrupción.
- Determinar si se adelantaron acciones de monitoreo.
- Revisar las acciones del monitoreo.