POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

TERMINAL METROPOLITANA DE TRANSPORTE DE BARRANQUILLA S.A.

AÑO 2019

Contenido

1. NTRODUCCIÓN.

El concepto de Administración del Riesgo se introduce en las entidades públicas debido a que todas las organizaciones, independientemente de su naturaleza, tamaño y objeto misional están expuestas a diversos riesgos o eventos que pueden poner en peligro su existencia, sus metas, su plan de desarrollo o estratégico institucional y hasta la oportunidad y eficacia de los servicios y bienes que ofrece.

Desde la perspectiva de la Norma Técnica **NTC-ISO 31000** e **ISO 9001** se considera que los sistemas de gestión se deben trabajar con un enfoque basado en riesgos que permita identificarlos y actuar con suficiente anticipación para evitar que sucedan o aminorar sus efectos. La administración de riesgos es la base para la planificación, que debe contribuir al logro de los objetivos institucionales; además permite identificar, analizar y abordar los hechos que se presenten para adoptar estrategias o actividades que garanticen cumplir con la misión, la visión y la entrega de bienes y servicios con calidad por parte de la entidad.

La Terminal Metropolitana de Transportes de Barranquilla S.A. define su política de Administración del riesgo tomando como referentes: (i) los parámetros establecidos en el Modelo Integrado de Planeación y Gestión MIPG, (ii) así como los del Modelo Estándar de Control Interno en lo referente a las líneas de defensa, (iii) los lineamientos de la Guía para la administración del riesgo de la Función Pública versión 4.0 (2018) que articula los riesgos de gestión, los de corrupción y los de seguridad digital y fortalece el diseño de controles.

La administración del riesgo es liderada por la Alta Dirección y ejecutada por los responsables de los diez (10) procesos institucionales con los que cuenta la Terminal Metropolitana de Transportes de Barranquilla S.A. y, demanda la participación y compromiso de los funcionarios y trabajadores de la entidad, **de modo que todos los procesos y dependencias** deben cumplir los lineamientos aquí enunciados para la identificación, análisis, valoración y tratamiento de los riesgos que puedan afectar la misión y el cumplimiento de los objetivos institucionales, en el marco de los programas, proyectos, planes, procesos y productos de la TTBAQ mediante:

a) La identificación y documentación de riesgos de gestión, de corrupción y de seguridad en cada proceso de la entidad,
b) El establecimiento de acciones de control preventivas para los riesgos identificados y,
c) La actuación correctiva y oportuna ante una eventual materialización de los riesgos.

Para administrar adecuadamente los riesgos de gestión y corrupción, la Terminal Metropolitana de Transportes de Barranquilla S.A. adopta los lineamientos de la guía de la Función Pública para la gestión del riesgo (2018. Versión 4) y, la hará efectiva a través de la herramienta diseñada por la entidad con apoyo de la Fundación Centro de Estudios Innovación Atlántico FUNCESIA denominada "*Herramienta_Mapa_de_Riesgo_de_Corrupción_TTBAQ".*

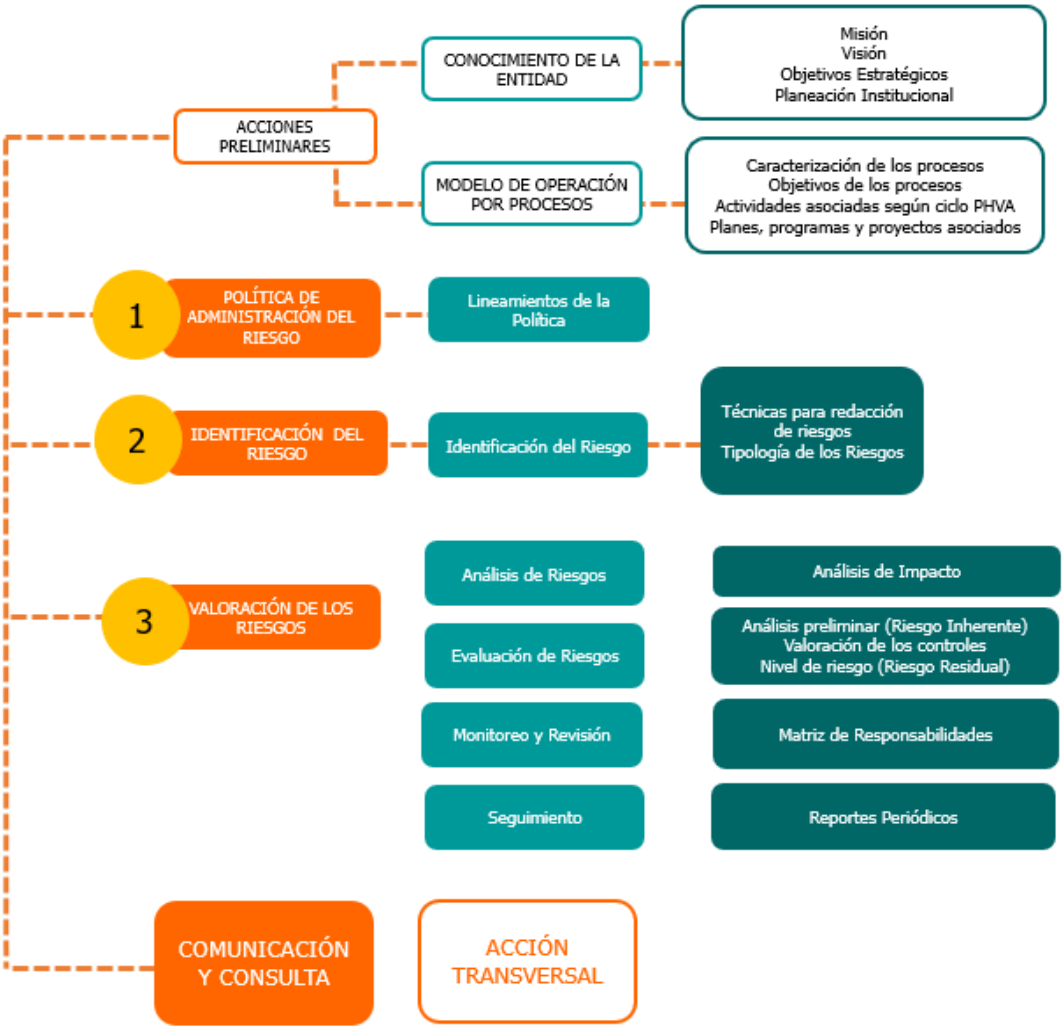
La entidad debe diseñar los instrumentos para gestionar los riesgos de gestión y los residuales.

La Oficina de Planeación y Presupuesto será la encargada de monitorear el cumplimiento de las acciones o ejecución de controles inherentes a la administración del riesgo junto con los responsables de procesos, en tanto que la Oficina de Control Interno será la encargada de realizar seguimiento a los riesgos conceptuando sobre si ocurrieron o no, la efectividad de los controles y, promoviendo las acciones correctivas a que haga lugar para subsanar las deficiencias y para adelantar las investigaciones que correspondan.

2. OBJETIVOS DE LA POLÍTICA.

Establecer disposiciones y criterios institucionales que brinden a la Terminal Metropolitana de Transportes de Barranquilla S.A. una adecuada identificación, análisis, valoración, administración y control de los riesgos que puedan afectar la misión y el logro de los objetivos institucionales.

3. METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO



4. ROLES INSTITUCIONALES (Líneas de Defensa)

4.1. Línea de Defensa Estratégica

Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento, está a cargo de la **Alta dirección y el Comité institucional de coordinación de control interno "CCCI"**.

Responsable: Alta Dirección y Comité Coordinador de Control Interno Institucional "CCCI".

ROLES:

- Establecer objetivos institucionales alineados con el propósito fundamental, metas y estrategias de la entidad.
- Establecer la Política de Administración del Riesgo.
- Asumir la responsabilidad primaria del SCI y de la identificación y evaluación de los cambios que podrían tener un impacto significativo en el mismo.
- Revisar los cambios en el "Direccionamiento estratégico" y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados.
- Revisión del adecuado desdoblamiento de los objetivos institucionales a los objetivos de procesos, que han servido de base para llevar a cabo la identificación de los riesgos.
- Hacer seguimiento -Comité Institucional y de Control Interno- a la implementación de las etapas de la gestión del riesgo y a los resultados de las evaluaciones realizadas por Control Interno o Auditoría Interna.
- Revisar el cumplimiento a los objetivos institucionales y de procesos y sus indicadores e identificar, en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos.

- Revisar, por lo menos trimestralmente, los informes sobre los riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que los ocasionaron.

- Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar, en lo posible, la repetición del evento.

4.2. Primera Línea de Defensa

Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, aplicación, monitoreo y acciones de mejora.

Responsable: Líderes de los Procesos Institucionales

ROLES:

- Identificar y valorar los riesgos que pueden afectar el logro de los objetivos institucionales.

- Definir y diseñar los controles a los riesgos.

- A partir de la política de administración del riesgo, establecer sistemas de gestión de riesgos y las responsabilidades para controlar riesgos específicos bajo la supervisión de la alta dirección.

- Construir los mapas de riesgos por procesos.

- Identificar y controlar los riesgos relacionados con posibles actos de corrupción en el ejercicio de sus funciones y el cumplimiento de sus objetivos, así como en la prestación del servicio y/o relacionados con el logro de los objetivos.

- Identificar, disuadir y detectar fraudes, y revisar con el auditor interno de la entidad la exposición de la entidad al fraude.

- Revisar los cambios en el Direccionamiento Estratégico o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de sus procesos.

- Revisar el que diseño y ejecución de los controles establecidos para la mitigación de los riesgos sea adecuado y eficaz.

- Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos.

- Revisar el cumplimiento de los objetivos de sus procesos a través de sus indicadores de desempeño, e identificar en caso de que no se estén cumpliendo, los riesgos que están ocurriendo.

- Revisar y reportar a Planeación, los riesgos que se han materializado en la entidad, incluyendo los de corrupción, así como las causas que los originaron.

- Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento y lograr el cumplimiento a los objetivos.

- Revisar y hacer seguimiento al cumplimiento de las actividades y planes de acción acordados con la línea estratégica, segunda y tercera línea de defensa con relación a la gestión de riesgos.

4.3. Segunda Línea de Defensa

Apoya y guía la línea estrategia y la primera línea de defensa en la gestión adecuada de los riesgos que pueden afectar el cumplimiento de los objetivos institucionales y sus procesos, a través de directrices para identificar, analizar, evaluar y tratar los riesgos. Lleva un monitoreo independiente al cumplimiento de las etapas de la gestión de riesgos.

Responsables: Oficina de planeación y presupuesto, servidores responsables de monitoreo y evaluación de controles, supervisores y miembros de comités en la entidad.

ROLES:

- Monitorear periódicamente el cumplimiento de las acciones asociadas al control o ejecución de controles a través de la solicitud de gestión de indicadores de los diferentes procesos.

- Revisar los cambios en el direccionamiento estratégico o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de actualizar los controles de los riesgos.

- Revisar el diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y formular recomendaciones para el fortalecimiento de los mismos.

- Determinar que las actividades de control para la mitigación de los riesgos se documenten.

- Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar que vuelva a ocurrir.

- Contar con un esquema de monitoreo en cada uno de los procesos, sobre la ejecución de los controles.

- Elaborar informes consolidados para las diversas partes interesadas sobre las actividades de monitoreo realizadas.

- Hacer seguimiento a los resultados de las acciones emprendidas para mitigar los riesgos, cuando haya lugar a ello.

- Los supervisores e interventores de contratos deben realizar seguimiento a los riesgos de estos y generar las alertas respectivas.

4.4. Tercera Línea de Defensa

Provee aseguramiento (evaluación) independiente y objetivo sobre la efectividad del sistema de gestión de riesgos, validando que la línea estratégica, la primera y segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos para el logro en el cumplimiento de los objetivos institucionales y del proceso.

Responsable: Oficina de Control interno

ROLES:

- Evaluar la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos.

- Hacer seguimiento objetivo a las áreas no cubiertas por la segunda línea de defensa.

- Asesorar, en coordinación con la oficina de planeación y presupuesto, sobre la identificación de los riesgos institucionales y el diseño de controles.

- Llevar a cabo el seguimiento a los riesgos consolidados en los mapas de riesgos de conformidad con el Plan Anual de Auditoria y reportar los resultados al “CCCI”.

- Recomendar mejoras a la política de administración del riesgo.

- Identificar y evaluar cambios que podrían tener un impacto significativo en el Sistema de Control Interno, durante las evaluaciones periódicas de riesgos y en el curso de las auditorías internas.

- Revisar la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo vinculadas a riesgos claves de la entidad.

- Alertar sobre la probabilidad de riesgo de fraude o corrupción en las áreas auditadas.

- Revisar los cambios en el “Direccionamiento estratégico” o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados, con el fin de que se formulen ajustes o mejoras.

- Revisar que se hayan identificado los riesgos que afectan en el cumplimiento de los objetivos de los procesos, además de incluir los riesgos de corrupción.

- Revisar el adecuado diseño y ejecución de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de los mismos.

- Revisar que las acciones orientadas a mitigar los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos y los planes de mejora, además, que se lleven a cabo de manera oportuna, se establezcan las causas y se evite, en lo posible, la repetición de hallazgos y la materialización de los riesgos.

5. ASPECTOS PRELIMINARES.

Antes de iniciar con la administración del riesgo se debe tener pleno conocimiento sobre la operación de la entidad, para ello resulta indispensable analizar su modelo de operación por procesos, los objetivos estratégicos, la misión, visión y caracterización de los procesos.

Los riesgos deben ser gestionados por procesos de acuerdo con el mapa de procesos, y estar asociados a las acciones relacionadas en la Caracterización de cada proceso y a sus objetivos.

5.1. TERMINOS Y DEFINICIONES

Administración del Riesgo: Actividad encaminadas a la intervención de los riesgos de la entidad, a través de la identificación, valoración, evaluación, manejo y monitoreo de los mismos de forma que se apoye el cumplimiento de los objetivos de la entidad.

Análisis de Riesgos: Determinación del impacto en función de la consecuencia o efecto y de la probabilidad de ocurrencia del riesgo.

Consecuencias: Hechos o acontecimientos que se derivan o resultan de la ocurrencia o la materialización de un riesgo.

Causas: Medios, circunstancias, situaciones o agentes generadores del evento.

Control: Acciones encaminadas a reducir la probabilidad de ocurrencia o el impacto que pueda generar la materialización del riesgo.

Evento: Hecho que se genera durante la gestión de un proceso afectando el logro del objetivo del mismo, tiene relación directa con las actividades críticas de los planes operativos, las actividades de ruta crítica de los Proyectos de Inversión y las actividades críticas de control de los procesos.

Frecuencia: Periodicidad con que ha ocurrido un evento.

Gestor del Riesgo: Funcionario líder de la dependencia, quien apoya al responsable del riesgo.

Identificación del Riesgo: Descripción de la situación no deseada.

Impacto: Magnitud de las consecuencias que pueden ocasionar a la entidad la materialización del riesgo.

Mapa de riesgos: Herramienta metodológica que permite hacer un inventario de los riesgos por proceso, haciendo la descripción de cada uno de ellos, las posibles consecuencias y su forma de tratamiento.

Políticas de manejo del Riesgo: Son los criterios que orientan la toma de decisiones para tratar, y en lo posible minimizar, los riesgos en la entidad, en función de su evaluación.

Probabilidad: Medida para estimar la posibilidad de que ocurra un evento.

Responsable del riesgo: Es el encargado de identificar, valorar y definir el plan de contingencia, el manejo y monitoreo para cada uno de los riesgos del proceso bajo su responsabilidad.

Riesgo: Posibilidad de ocurrencia del evento que tiene un efecto positivo o negativo sobre el producto o servicio generado de un proceso o el cumplimiento de los objetivos institucionales.

Riesgo residual: Es aquel que continúa aún después de aplicar controles para mitigar el riesgo

Riesgo Inherente: Es el riesgo puro, al cual no se han aplicado controles, para controlarlo y buscar evitar su materialización.

Tratamiento: Opciones que determinan el tipo de acciones a implementar para administrar el riesgo.

Valoración: Grado de exposición al riesgo con la clasificación de probabilidad e impacto aplicando los controles existentes.

6. IDENTIFICACIÓN DEL RIESGO.

La identificación del riesgo se realiza a partir de la descripción de los eventos o situaciones que pueden entorpecer el normal desarrollo de los objetivos del proceso con base en el contexto interno y externo. Es necesario hacer una breve descripción del riesgo refiriéndose a sus características o las formas en que se manifiesta.

La identificación del riesgo **le corresponde a la primera línea de defensa**. En esta primera fase se deben establecer las fuentes o factores de riesgo, los eventos o riesgos, sus causas y sus consecuencias. Para el análisis se pueden involucrar

datos históricos, análisis teóricos, opiniones informadas y expertas y las necesidades de las partes involucradas (NTC ISO31000, Numeral 2.15).

Para identificar un riesgo, sus causas y consecuencias, se sugiere formular las siguientes preguntas

¿ Qué puede ocurrir?
¿ Cómo puede ocurrir?
¿ Por qué puede ocurrir?
¿ Qué consecuencias tendría su materialización?

6.1. Identificación de Riesgos de Corrupción

Teniendo en cuenta que riesgo de corrupción se define como: "la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado", es necesario que en la descripción del riesgo concurran los siguientes elementos:

Es importante tener presente que los elementos de "Uso de Poder" y "Beneficio privado" son característicos del Riesgo de Corrupción, por lo que debe asegurarse que en la formulación de este tipo de riesgos se incluyan esos elementos.

El beneficio privado corresponde a la intensión de generar un lucro o beneficio a un tercero o para el mismo servidor público.

El uso del poder corresponde a la circunstancia de que un servidor público o particular en ejercicio de funciones públicas, haga uso de su cargo o de sus funciones para generar el hecho de corrupción.

6.2. Identificación de Activos.

Le corresponde a la primera línea de defensa identificar los activos en cada proceso. Un activo es cualquier elemento que tiene valor para la organización, sin embargo,

en el contexto de seguridad digital, **son activos que utiliza la organización para funcionar en el entorno digital**: aplicaciones de la organización, servicios web, redes, información física o digital, tecnologías de información -TI, tecnologías de operación -TO.

Se busca proteger los activos para garantizar tanto su funcionamiento interno como el funcionamiento de la entidad de cara al ciudadano, aumentando su confianza en el uso del entorno digital.

Para identificar los activos, se deben seguir los siguientes pasos:

7. VALORACIÓN DEL RIESGO.

Consiste en analizar el riesgo para establecer su probabilidad de ocurrencia y el nivel de consecuencias o impacto con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE); y posteriormente evaluarlo, para confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (RIESGO RESIDUAL).

7.1. Probabilidad

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 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.

Para su determinación se utiliza la tabla de probabilidad:

MEDICIÓN DE LA PROBABILIDAD DEL RIESGO			
Descriptor	**DESCRIPCIÓN**	**FRECUENCIA**	**NIVEL**
Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales)	No se ha presentado en los últimos 5 años.	**1**
Improbable	El evento puede ocurrir en algún momento	Se presentó al menos una vez en los últimos 5 años	**2**
Posible	El evento podría ocurrir en algún momento	Se presentó al menos una vez en los últimos 2 años.	**3**
Probable	Es viable que el evento ocurra en la mayoría de las circunstancias	Se presentó al menos una vez en el último año.	**4**
Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Se ha presentado más de una vez al año.	**5**

7.2. Impacto

Por **IMPACTO** se entienden las consecuencias que puede ocasionar la ocurrencia del riesgo. Para su determinación de acuerdo con el tipo de riesgo, se utilizan los siguientes criterios o tablas.

7.2.1. Impacto de riesgos de gestión

NIVEL	VALOR	IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
CATASTRÓFICO	5	- 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 la entidad.	- 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 puede recuperar. - 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	4	- 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 operaciones de 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	3	- 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 la entidad	- 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	2	- 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 presupuesto general 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	1	- 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

Fuente: Adaptado del Instituto de Auditores Internos. COSO ERM. Agosto 2004.

7.2.2. Impacto de riesgos de corrupción

El impacto se determina respondiendo objetivamente 19 preguntas relacionadas con los efectos que puede causar el riesgo.

Al responder afirmativamente de UNA a CINCO preguntas(s) se genera un impacto moderado; de SEIS a ONCE genera un impacto MAYOR, de DOCE a DIECINUEVE un impacto catastrófico.

La pregunta 11 se refiere a que la conducta sea objeto de Sanciones como amonestaciones, multas, reconvenciones distintas a las penales y disciplinarias.

No	Pregunta: si el riesgo de corrupción se materializa podría...	SI	NO
1	¿Afecta al grupo de funcionarios del proceso?		
2	¿Afecta 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?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		

MODERADO	Genera medianas consecuencias sobre la entidad
MAYOR	Genera altas consecuencias sobre la entidad
CATASTRÓFICO	Genera consecuencias desastrosas para la entidad

Fuente: Secretaría de Transparencia de la Presidencia de la República

7.2.3. Impacto de riesgos de seguridad digital

El impacto de los Riesgos de seguridad digital se determinan con los siguientes criterios:

NIVEL	VALOR	IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
CATASTRÓFICO	5	- Afectación ≥X% de la población. - Afectación ≥X% del presupuesto anual de la entidad. - Afectación muy grave del medio ambiente que requiere de ≥X años de recuperación	- Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. - Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. - Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.
MAYOR	4	- Afectación ≥X% de la población. - Afectación ≥X% del presupuesto anual de la entidad. - Afectación importante del medio ambiente que requiere de ≥X meses de recuperación.	- Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. - Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. - Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.
MODERADO	3	- Afectación ≥X% de la población. - Afectación ≥X% del presupuesto anual de la entidad. - Afectación leve del medio ambiente requiere de ≥X semanas de recuperación.	- Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. - Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. - Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros.
MENOR	2	- Afectación ≥X% de la población. - Afectación ≥X% del presupuesto anual de la entidad. - Afectación leve del medio ambiente requiere de ≥X días de recuperación	- Afectación leve de la integridad. - Afectación leve de la disponibilidad. - Afectación leve de la confidencialidad.

INSIGNIFICANTE	1	- Afectación ≥X% de la población. - Afectación ≥X% del presupuesto anual de la entidad. - No hay afectación medioambiental.	- Sin afectación de la integridad. - Sin afectación de la disponibilidad. - Sin afectación de la confidencialidad.

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones. 2017

Las variables **confidencialidad, integridad y disponibilidad** se definen de acuerdo con el modelo de seguridad y privacidad de la información de la estrategia de Gobierno Digital (GD) del Ministerio de Tecnologías de la Información y las Comunicaciones.

La variable **población** se define teniendo en cuenta el contexto externo de la entidad; es decir, que la población está asociada a las personas a las que se les prestan servicios o trámites en el entorno digital, y que de una u otra forma, pueden verse afectadas por la materialización de algún riesgo. Los porcentajes en las escalas pueden variar, según la entidad y su contexto.

La variable **presupuesto** es la consideración de presupuesto afectado por la entidad debido a la materialización del riesgo, contempla sanciones económicas o impactos directos en la ejecución presupuestal.

La variable **ambiental** está relacionada con la afectación del medio ambiente por la materialización de un riesgo de seguridad digital. Esta variable puede no ser utilizada en la mayoría de los casos, pero debe tenerse en cuenta, ya que en alguna eventualidad puede existir afectación ambiental.

7.3. Mapa de Calor

Para calcular el riesgo inherente se tomará la zona o calificación que resulte de la intersección entre la probabilidad y el impacto según la siguiente tabla:

Resultados de la calificación del Riesgo						
Probabilidad	Puntaje	Zonas de Riesgo				
Casi seguro	5	Zona Alta	Zona Alta	Zona Extrema	Zona Extrema	Zona Extrema
Probable	4	Zona Moderada	Zona Alta	Zona Alta	Zona Extrema	Zona Extrema
Posible	3	Zona Baja	Zona Moderada	Zona Alta	Zona Extrema	Zona Extrema
Improbable	2	Zona Baja	Zona Baja	Zona Moderada	Zona Alta	Zona Extrema
Rara vez	1	Zona Baja	Zona Baja	Zona Moderada	Zona Alta	Zona Extrema
Impacto		Insignificante	Menor	Moderado	Mayor	Catastrófico
Puntaje		**1**	**2**	**3**	**4**	**5**

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.

8. EVALUACIÓN DE RIESGO.

La evaluación del riesgo está dirigida a confrontar los resultados del Riesgo inicial (**RIESGO INHERENTE**) frente a los controles establecidos con el fin de determinar la zona de riesgo final (**RIESGO RESIDUAL**).

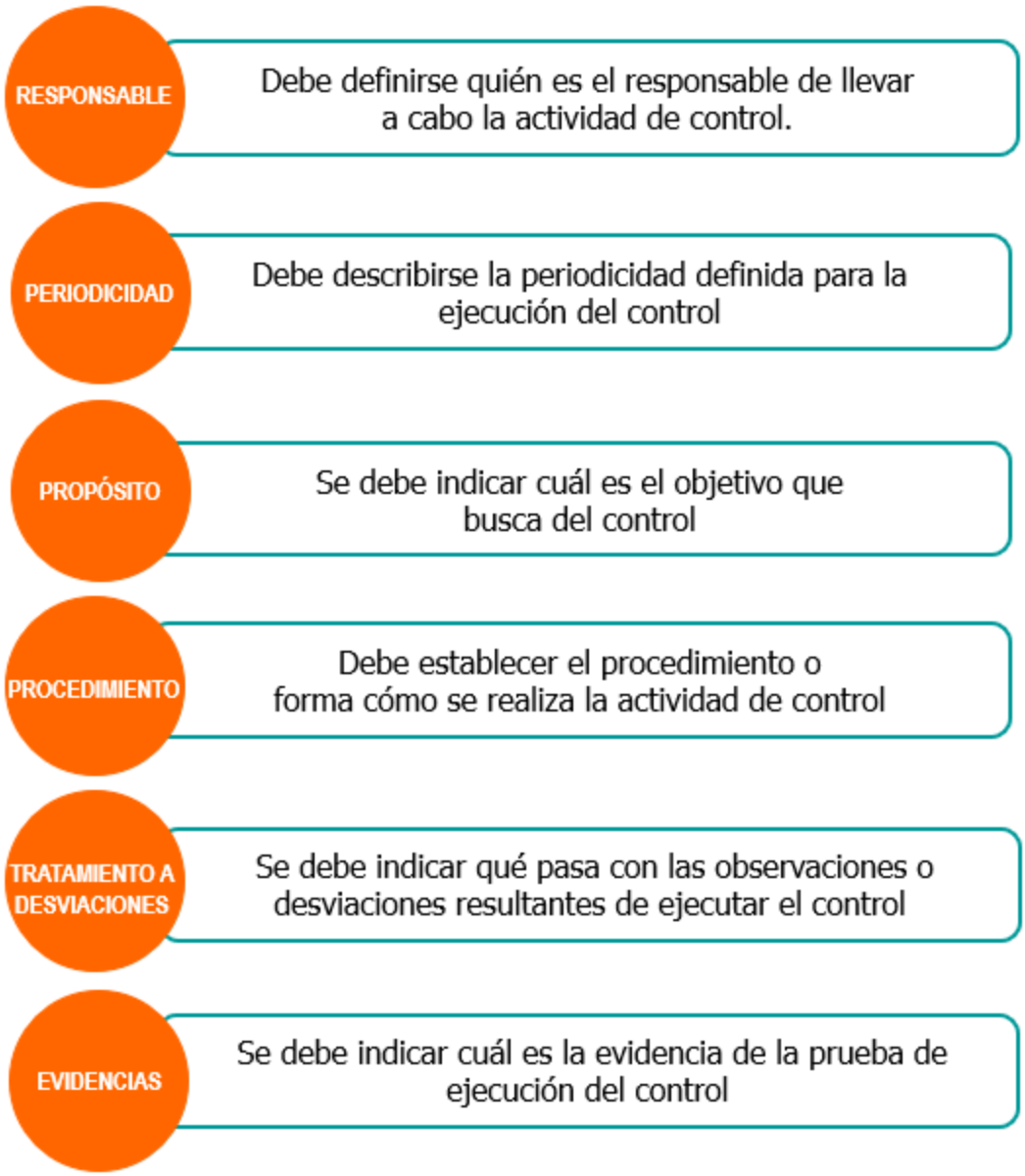
En ese sentido, se busca establecer controles dirigidos a la administración del riesgo y posteriormente valorarlos. Se deben seguir las siguientes acciones:

- Identificar los riesgos inherentes o subyacentes que pueden afectar el cumplimiento de los objetivos estratégicos y de proceso.
- Identificar las causas o fallas que pueden dar origen a la materialización del riesgo.
- Para cada causa se debe asignar un control.

- Evaluar si los controles están dirigidos a evitar o mitigar el riesgo.

8.1. Diseño de Controles

Para diseñar un control (acciones preventivas, correctivas o detectivas de los riesgos) debemos utilizar los siguientes **Criterios:**



- **RESPONSABLE:** Persona asignada para ejecutar el control. Debe tener la autoridad, competencias y conocimientos para ejecutar el control dentro del proceso. Las responsabilidades pueden ser distribuidas entre varios individuos.

  Si la PERSONA o responsables cumplen esos criterios, quiere decir que el control está bien diseñado, si la respuesta es negativa, tenemos que identificar la situación y mejorar el diseño del control con relación a la persona responsable de su ejecución.

  Controles sistematizados. Cuando el control lo hace un sistema o una aplicación de manera automática a través de un sistema programado, es importante establecer como responsable de ejecutar el control al sistema o aplicación.

- **PERIODICIDAD:** El control debe tener una periodicidad específica para su realización (diario, mensual, trimestral, anual, permanente etc.) y su ejecución debe ser consistente y oportuna para la mitigación del riesgo.

  Cada vez que se diseña un control debemos preguntarnos si la periodicidad en que este se ejecuta ayuda a prevenir o detectar el riesgo de manera oportuna. Si la respuesta es SÍ, entonces la periodicidad del control está bien diseñada.

- **PROPÓSITO**: 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 (verificar, validar, conciliar, comparar, revisar, cotejar) o detectar la materialización del riesgo, con el objetivo de llevar acabo los ajustes y correctivos en el diseño del control o en su ejecución.

  El solo hecho de establecer un procedimiento o contar con una política por sí sola no previene o detecta un riesgo.

- **PROCEDIMIENTO:** El control debe indicar el cómo se realiza, de tal forma que se pueda evaluar si la fuente u origen de la información que sirve para ejecutar el control, es confiable para la mitigación del riesgo. Cuando estemos evaluando el control debemos preguntarnos si la fuente de información utilizada es confiable. Ej.: para verificar los requisitos que debe cumplir un proveedor en el momento de ser contratado es mejor utilizar una lista de chequeo que hacerlo de memoria, dado que se nos puede quedar algún requisito por fuera.

- **TRATAMIENTO A DESVIACIONES:** El control debe indicar qué hacer cuando se detecten desviaciones al ejecutar el control; de tal manera que al evaluar si un control está bien diseñado, debe asegurarse que se expongan las actividades que realizará la entidad para gestionar oportunamente los correctivos.

- **EVIDENCIA**: Debe quedar una evidencia de la ejecución del control. Esta evidencia ayuda a que se pueda revisar lo actuado por parte de un tercero y llegue a la misma conclusión de quien ejecutó el control, respecto de que fue ejecutado de acuerdo con los siguientes parámetros:

  a. Fue realizado por el responsable que se definió.
  b. Se realizó de acuerdo a la periodicidad definida.
  c. Se cumplió con el propósito del control.
  d. Se dejó la fuente de información que sirvió de base para su ejecución.
  e. Hay explicación a las observaciones o desviaciones resultantes de ejecutar el control.

8.2. Clasificación de los Controles

Nuestros controles se clasifican en PREVENTIVOS y DETECTIVOS.

A. Controles Preventivos: son aquellos que están diseñados para evitar un evento no deseado. Este tipo de controles buscan evitar la ocurrencia de los riesgos.

B. Controles Detectivos: están diseñados para identificar un evento o resultado no previsto después de que se haya producido. Buscan detectar la situación no deseada para que se corrija y se tomen las acciones correspondientes**.**

8.3. Valoración de Controles

Los criterios para el análisis y evaluación del diseño del control son seis (6):

Criterio de evaluación	Aspecto a evaluar en el diseño del control	Opciones de respuesta	
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
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
Propósito	¿Las actividades que se desarrollan en el control realmente buscan prevenir o detectar las causas que pueden dar origen al riesgo, Ej.: verificar, validar, cotejar, comparar, revisar, etc.?	Prevenir o detectar	No es un control
¿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
¿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
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

Peso o participación de cada variable en el diseño del control para la mitigación del riesgo

CRITERIO DE EVALUACIÓN	OPCIÓN DE RESPUESTA AL CRITERIO DE EVALUACIÓN	PESO
Asignación del responsable	Asignado	15
	No Asignado	0
Segregación y autoridad del responsable	Adecuado	15
	Inadecuado	0
Periodicidad	Oportuna	15
	Inoportuna	0
Propósito	Prevenir	15

	Detectar	10
	No es un control	0
Cómo se realiza la actividad de control	Confiable	15
	No confiable	0
Qué pasa con las observaciones o desviaciones	Se investigan y resuelven oportunamente	15
	No se investigan y resuelven oportunamente	0
Evidencia de la ejecución del control	Completa	10
	Incompleta	5
	No existe	0

Resultados de la evaluación del diseño del control

RANGO DE CALIFICACIÓN DEL DISEÑO	RESULTADO - PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL
Fuerte	Calificación entre 96 y 100
Moderado	Calificación entre 86 y 95
Débil	Calificación entre 0 y 85

Si las calificaciones del control, o el promedio del diseño de los controles está por debajo de 96%, se deben ajustar o mejorar los controles hasta que queden bien diseñados.

Calificación de la solidez del conjunto de controles

Se deben promediar todos los controles correspondientes a un riesgo, de acuerdo con las causas identificadas, y el resultado será el valor que afecte el riesgo inherente para el establecimiento del riesgo residual.

Desplazamiento del riesgo inherente para calcular el 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 con la siguiente tabla:

CRITERIO	SI EL CONTROL AYUDA A DISMINUIR LA PROBABILIDAD	SI EL CONTROL AYUDA A DISMINUIR IMPACTO
SOLIDEZ DEL CONJUNTO DE LOS CONTROLES	# 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	2	2
MODERADO	1	1

*Si la solidez del conjunto de los controles es débil, este no disminuirá ningún cuadrante de impacto o probabilidad asociado al riesgo

*Tratándose de riesgos de corrupción únicamente hay disminución de probabilidad; es decir, para el impacto no opera el desplazamiento.

9. TRATAMIENTO DEL RIESGO

Es tratamiento del riesgo es la respuesta establecida por **la primera línea de defensa** para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción.

El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

a. **Aceptar el Riesgo**: no se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (**Ningún riesgo de corrupción podrá ser aceptado**).

b. **Reducir el Riesgo**: se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general implica diseñar controles.

c. **Evitar el Riesgo**: se abandonan las actividades que dan lugar al riesgo; es decir, no iniciar o no continuar con la actividad que lo provoca.

d. **Compartir el Riesgo**: se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad

10. MONITOREO Y REVISIÓN

El monitoreo y revisión debe asegurar que las acciones establecidas en los mapas de riesgo se están llevando a cabo y evaluar la eficacia en su implementación, **adelantando revisiones** sobre la marcha para evidenciar todas aquellas situaciones o factores que pueden influir en la aplicación de acciones preventivas.

El monitoreo está a cargo de:

A. RESPONSABLES DE LOS PROCESOS Y JEFE DE PLANEACIÓN Y PRESUPUESTO:

Encargados de cumplir las **acciones asociadas a los controles** establecidos para cada uno de los riesgos identificados para su proceso, en la periodicidad establecida esta Política de administración del riesgo de la entidad.

Durante la aplicación de las acciones de seguimiento cada líder de proceso debe mantener los soportes que evidencian su aplicación para garantizar que dichos riesgos no ocurran y por ende que los objetivos del proceso se cumplirán.

La Jefe de Planeación y Presupuesto realizará actividades de monitoreo periódicas.

B. OFICINA DE CONTROL INTERNO:

Encargada de realizar el seguimiento a los riesgos consolidados. En sus procesos de auditoría interna dicha oficina debe analizar el diseño e idoneidad de los controles, determinando si son o no adecuados para prevenir o mitigar los riesgos de los procesos, si se aplicaron oportuna y adecuadamente, si se dejaron evidencias de su aplicación, y si se reportaron las desviaciones detectadas, haciendo uso de las técnicas relacionadas con pruebas de auditoría que permitan determinar la efectividad de los controles.

Los informes de control interno deben contener recomendaciones que promuevan ajustes, mejoras o actividades para subsanar las desviaciones detectadas.

11. LINEAMIENTOS PARA LOS RIESGOS MATERIALIZADOS

Si dentro del seguimiento realizado, bien sea por parte de la Oficina de Control Interno, la jefe de planeación y presupuesto o por los líderes de los procesos, se detecta que ocurrido uno o más riesgos, se debe:

A. POR PARTE DE LA OFICINA DE CONTROL INTERNO

Si el riesgo es de corrupción

- Convocar al Comité Coordinador de Control Interno e informar sobre los hechos detectados, desde donde se tomarán las decisiones para iniciar la investigación de los hechos.

- Dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante el ente de control respectivo.

- Facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos y sus controles asociados.

- Verificar que se tomaron las acciones y se actualizó el mapa de riesgos.

Si el riesgo es de gestión o de seguridad digital y se encuentra en las ZONAS: EXTREMA, ALTA O MODERADA.

- Informar al líder del proceso sobre el hecho encontrado.

- Orientar al líder del proceso para que realice la revisión, análisis y acciones correspondientes para resolver el hecho.

- Verificar que se tomaron las acciones y que se actualizó el mapa de riesgos correspondiente.

- Convocar al Comité Coordinador de Control Interno e informar sobre la actualización realizada.

Si el riesgo es de gestión o de seguridad digital y se encuentra en las ZONA BAJA:

- Aplicar las orientaciones de la política de riesgos institucional. (Verificar los niveles de aceptación del riesgo).

A. POR PARTE DE LOS LÍDERES DE LOS PROCESO U OTROS FUNCIONARIOS QUE PARTICIPAN O INTERACTÚAN CON EL PROCESO.

Si el riesgo es de corrupción

- Informar a la Alta Dirección sobre el hecho encontrado.

- De considerarlo necesario, realizar la denuncia ante el ente de control respectivo.
- Iniciar con las acciones correctivas necesarias.
- Realizar el análisis de causas y determinar acciones preventivas y de mejora.
- Análisis y actualización del mapa de riesgos.

Si el riesgo es de gestión o de seguridad digital y se encuentra en las ZONAS: EXTREMA, ALTA O MODERADA.

- Promover las acciones correctivas necesarias, dependiendo del riesgo materializado.
- Identificar las causas y determinar acciones preventivas y de mejora.
- Analizar y actualizar el mapa de riesgos.
- Informar a la Alta Dirección sobre el hallazgo y las acciones tomadas.

Si el riesgo es de gestión o de seguridad digital y se encuentra en las ZONA BAJA

- Aplicar las orientaciones de la política de riesgos institucional. (*Verificar los niveles de aceptación del riesgo*).

De acuerdo con el seguimiento realizado es importante determinar, *al final de cada vigencia,* si los mapas de riesgos deben ser actualizados o si se mantienen bajo las mismas condiciones en cuanto a factores de riesgo, identificación, análisis y valoración del riesgo.

Para poder determinarlo se analizará si no se han presentado hechos significativos como son:

- Riesgos materializados relacionados con posibles actos de corrupción.
- Riesgos de gestión materializados en cualquiera de los procesos.

- Observaciones o hallazgos por parte de la Oficina de Control Interno o bien por parte de un ente de control, respecto de la idoneidad y efectividad de los controles.

- Cambios importantes en el entorno estratégico o normativo que puedan generar nuevos riesgos.

- Inclusión de nuevos riesgos o controles identificados por la entidad.

No obstante, los mapas de riesgos deben ser flexibles y permitir cambios cuando se requieran.

REFLEXIÓN: La aplicación de la política de administración de riesgos involucra a todos los actores de la entidad, en todos los niveles, cada uno con un rol diferente pero convergente en evitar que los riesgos sucedan o en mitigar sus efectos, de tal manera que es imprescindible que esta política sea conocida por todos, entendida y aplicada en el quehacer diario, pero sobre todo, que sea monitoreado su cumplimiento por parte del área de Planeación y de Control interno.