CONTROL DE CAMBIOS		
VERSIÓN	**FECHA**	**DESCRIPCIÓN DE LA MODIFICACIÓN**
1	14/08/2015	Versión inicial del documento
2	27/03/2017	Cambio en el mapa de procesos de la Entidad
3	03/04/2019	Cambio de tipo documental de Instructivo (IN) a Guía (GU) y cambio del código del documento por integración al Proceso de Direccionamiento Estratégico; cambio del mapa de Procesos de la Entidad.
4	19/08/2020	Cambio de nombre del documento, inclusión de gestión de riesgos de seguridad de la información, inclusión del riesgo de soborno y ajustes generales de redacción del documento.
5	13/05/2021	Actualización de la Metodología con base en la versión 5 de la *Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP*, que modificó las definiciones de algunos términos, los criterios de valoración de probabilidad e impacto de los riesgos, y de evaluación de los controles para los riesgos estratégicos, de gestión y de seguridad de la información. Ajuste de las responsabilidades de la línea estratégica y las tres líneas de defensa de conformidad con el *Manual operativo MIPG, versión 4.*

Elaboró	Revisó	Aprobó
LISBETH LORENA MURILLO PARDO Profesional Universitario 219-01 (e) Dirección de Planeación	HÉCTOR HERNÁN GONZÁLEZ NARANJO Director de Planeación	HÉCTOR HERNÁN GONZÁLEZ NARANJO Director de Planeación

TABLA DE CONTENIDO

1. OBJETIVO

Establecer las directrices generales para la administración de los riesgos estratégicos, de gestión, de seguridad de la información y de corrupción en la Personería de Bogotá, D. C., que puedan afectar el logro de la misión, visión y los objetivos de la Entidad, de acuerdo con la Política de Administración del Riesgo vigente.

2. ALCANCE

La presente Guía aplica a todos los procesos de la Personería de Bogotá, D. C., inicia con la identificación y/o actualización del contexto estratégico institucional y por procesos de la Entidad, y finaliza con el seguimiento y evaluación de los controles y planes de tratamiento definidos para la gestión de los riesgos identificados.

3. RESPONSABLES

La gestión de los Riesgos en la Personería de Bogotá, D. C. es responsabilidad de todos(as) los(as) servidores(as) de la Entidad, quienes tienen roles y responsabilidades diferentes, de acuerdo con lo establecido en cada **línea de defensa**, las cuales se encuentran detalladas en la etapa de *Monitoreo y revisión* de la presente guía, de conformidad con lo establecido en la Dimensión 7 del Manual Operativo del Modelo Integrado de Gestión MIPG – V4.

4. DEFINICIONES

Las definiciones utilizadas corresponden a las contenidas en la “Guía para la administración del riesgo y el diseño de controles en entidades públicas”, versión 5, del Departamento Administrativo de la Función Pública - DAFP, 2020.

- **Administración y/o Gestión del Riesgo:** es un proceso efectuado por la alta dirección de la Entidad y por todo el personal, con el propósito de proporcionar a la administración el aseguramiento razonable con respecto al logro de los objetivos.

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

- **Alta Dirección:** Persona o grupo de personas que dirige y controla una organización al más alto nivel. En la Personería de Bogotá, D.C. la alta dirección está compuesta por los miembros del Comité Institucional de Gestión y Desempeño, quienes tienen responsabilidades específicas frente a la gestión del riesgo.

- **Amenaza:** situación o evento potencial que constituye una posible materialización de un incidente no deseado, el cual puede ocasionar afectación a la seguridad de la información institucional.

- **Análisis de Riesgo:** actividad que busca establecer la probabilidad de ocurrencia del riesgo y su o impacto, con el fin de estimar la zona de riesgo inicial**.**

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

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

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

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

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

- **Código de integridad:** Documento en el cual se describen valores que reflejan mínimos de integridad a ser aplicados por los servidores públicos (DAFP, 2017, p. 27) y que se desarrolla en una infraestructura de integridad institucional como códigos y políticas antisoborno y de conflictos de intereses, entre otras (DAFP, 2017, p. 28).

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

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

- **Control Correctivo:** Control accionado en la salida del proceso y después de que se materializa el riesgo, estos controles tienen costos implícitos. Atacan el impacto generado por algún evento de riesgo.

- **Control Detectivo:** Control accionado durante la ejecución del proceso, estos controles detectan el riesgo pero generan reprocesos. Atacan la probabilidad de ocurrencia del riesgo.

- **Control Preventivo:** Control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado. Va a las causas del riesgo, atacan la probabilidad de ocurrencia del riesgo.

- **Consecuencia:** Resultado de un evento que afecta los objetivos[1]. Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

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

- **Evento:** es un riesgo materializado que puede dar origen al incumplimiento de los objetivos y metas de la entidad.

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

- **Gestores de integridad:** Grupo responsable de promover y liderar el proceso de implementación de la gestión de la integridad en la Personería de Bogotá, D.C., conformado por Resolución 330 de 2018.

- **Integridad**: propiedad que garantiza la exactitud y completitud de la información.

- **Inventario de Activos:** instrumento que permite identificar los activos de información a los que se les debe brindar mayor protección y que se requieren para servir a los propósitos de la Entidad.

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

- **Límite de aceptación del riesgo:** Es la zona del riesgo a partir de la cual el mismo se define inaceptable.

[1] Definición Norma ISO 31000:2016

- **Mapa de riesgos:** Documento que contiene la información resultante de cada una de las etapas de gestión del riesgo.

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

- **Objetivo:** Algo que se espera lograr o se pretende conseguir.

- **Oportunidad:** es una acción para minimizar un efecto negativo, que no sólo minimiza el efecto, sino que ayuda a que se logre de forma más eficaz algún resultado previsto. Es decir, las oportunidades pueden surgir a partir del análisis de los posibles controles que pueden aplicarse para minimizar los efectos negativos de un riesgo.

- **Perfil de Riesgo:** Descripción de un conjunto de riesgos. El conjunto de riesgos puede contener aquellos que se relacionan con la organización en su totalidad o con parte de ella.

- **Plan Anticorrupción y de Atención al Ciudadano - PAAC:** Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.

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

- **Punto de riesgo:** son actividades dentro del flujo del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.

- **Referente de Gestión:** Es el rol asignado a un(a) funcionario(a) o contratista en los diferentes procesos siendo el (la) encargado(a) de articular con los(as) responsables de dimensiones, sistemas de gestión y/o procesos el desarrollo

de actividades necesarias para la implementación, mantenimiento y sostenibilidad del Modelo Integrado de Planeación y Gestión- MIPG.

- **Riesgo:** El riesgo se define como la combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas. El riesgo se mide en términos de impacto y probabilidad.[2] Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.[3]

  Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos. (DAFP, 2020)

- **Riesgo Aceptable:** Riesgo que se encuentra en una zona en la cual se considera que los controles existentes son apropiados y por lo tanto no se requiere de una mayor intervención.

- **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.

- **Riesgo de Gestión:** Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos de la Entidad.

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

- **Riesgo Estratégico:** Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos 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, entre otros.

- **Riesgo Inaceptable:** Riesgo que se encuentra en una zona en la cual se considera que los controles existentes no son suficientes y por lo tanto debería emprenderse alguna acción de tratamiento del riesgo.

[2] Instituto Internacional de Auditores.

[3] Departamento Administrativo de la Función Pública, 2020

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

- **Riesgos Operativos:** Posibilidad de ocurrencia de eventos que afecten los procesos misionales de la Entidad.

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

- **Riesgos Tecnológicos:** Posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.

- **Soborno:** Cuando una persona da u ofrece "dinero u otra utilidad para que se realice u omita un acto propio del cargo de un funcionario público, o para que se ejecute uno contrario a sus deberes oficiales" [4]

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

- **Tratamiento de Riesgo:** respuesta establecida por la primera línea de defensa para la mitigación de los riesgos residuales identificados.

- **Valoración del Riesgo**: Proceso de determinación de la probabilidad de ocurrencia e impacto del riesgo, y determinación del valor de su combinación antes y después de aplicar controles.

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

5. NORMATIVIDAD APLICABLE Y OTROS DOCUMENTOS

- Decreto 1083 de 2015, artículo 2.2.21.5.4 - *Administración de riesgos*
- Decreto 1499 del 2017, artículo 2.2.22.3.8 - *Comité Institucional de Gestión y Desempeño*
- Decreto 648 del 2017, artículo 2.2.21.1.5 - *Comité Institucional de Coordinación de Control Interno*

[4] Metodología prevención Riesgos de Soborno en Entidades Púbicas – Veeduría Distrital 2019

- Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 4. Departamento Administrativo de la Función Pública - DAFP, 2018. - *Capítulo riesgos de Corrupción.*
- Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5. Departamento Administrativo de la Función Pública - DAFP, 2020.
- Manual operativo del Modelo Integrado de Planeación y Gestión – MIPG, versión 4. Departamento Administrativo de la Función Pública - DAFP, 2021.
- Metodología prevención de Riesgos de Soborno en entidades públicas. Veeduría Distrital, 2019.
- Norma ISO 31000 de 2018.
- Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas (Anexo Guía para la Administración del Riesgo DAFP 2020).
- Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas (Anexo Guía para la Administración del Riesgo DAFP 2020).

6. POLÍTICAS DE OPERACIÓN

6.1 La identificación de riesgos se hace a partir del contexto general de la Entidad, y del análisis de los objetivos estratégicos y de gestión de cada proceso.

6.2 El análisis de los riesgos debe realizarse de manera permanente y al menos una vez al año por los responsables y referentes de proceso, junto con su equipo de trabajo, verificando las causas que los originan y la efectividad de los controles y de las acciones implementadas para su reducción o mitigación.

6.3 En caso de que un proceso considere que un riesgo se encuentra totalmente controlado, se debe hacer un análisis para determinar si los puntos de control establecidos en sus procedimientos o demás documentos, permiten controlar de manera permanente algún evento de riesgo. Si este análisis conlleva a la eliminación de algún riesgo del proceso, esta decisión debe quedar documentada y ser informada a la Dirección Planeación para su análisis metodológico.

6.4 Al eliminar las causas que originan algún riesgo, y en caso de considerarlo necesario, el responsable de proceso, fundamentando su solicitud, debe

elevar consulta a la Segunda Línea de Defensa para determinar si el riesgo puede ser eliminado o no, del mapa de riesgos institucional.

6.5 Si durante el análisis de permanente de su entorno o en el monitoreo de sus riesgos, el responsable de proceso y su equipo de trabajo consideran necesaria la actualización de su mapa de riesgos, deben informar mediante comunicación escrita, a la Segunda Línea de Defensa sobre su decisión con el fin de determinar la viabilidad de cambio del mapa de riesgos institucional, previa sustentación por parte de los responsables o líderes de proceso.

6.6 Los responsables y/o referentes de proceso, antes del 15 de enero de cada vigencia, deben enviar su Mapa de Riesgos a la Dirección de Planeación para su revisión, consolidación y publicación, la cual se tiene realizar a más tardar el 31 de enero de cada anualidad.

6.7 Todos los riesgos contemplados en la vigencia anterior a la fecha de actualización del Mapa de Riesgos que se realiza al inicio de cada anualidad, deben continuar siendo controlados por cada proceso; es decir, no es posible eliminar los riesgos sin previo análisis por parte del proceso y consulta a la Dirección de Planeación, no obstante, es de aclarar que el responsable de proceso es autónomo de la decisión que tome al respecto.

6.8 Cada riesgo debe tener contemplada una acción de mejora o de reacción inmediata que pueda ejecutarse en caso de materializarse algún riesgo, con el fin de evitar altos niveles de impacto del evento y apoyar la toma de decisiones.

6.9 Corresponde al Comité Institucional de Coordinación del Sistema de Control Interno, someter a aprobación por parte del Representante Legal de la Entidad, la *Política de Administración del Riesgo* estructurada previamente por la Dirección de Planeación y presentada ante el Comité Institucional de Gestión y Desempeño.

6.10 En la presente guía, y de acuerdo con los lineamientos del DAFP (2020), las tablas de valoración de la probabilidad y del impacto, así como la matriz para la evaluación de los controles en los riesgos de gestión, estratégicos y de seguridad de la información, difieren de las tablas y matrices establecidas para los riesgos de corrupción.

6.11 La *evaluación de los controles* para los riesgos estratégicos, de gestión y de seguridad de la información, se realizará de manera acumulativa por cada uno de los controles existentes en cada riesgo identificado; de acuerdo con lo definido en la Guía para la administración de riesgos y diseño de controles del DAFP, 2020.

6.12 Con relación a los Riesgos de Corrupción se reitera que son inaceptables y que la valoración de su impacto después de controles, no cambia, es decir en caso de materializarse algún riesgo de corrupción, su impacto será el determinado en el riesgo inherente o inicial.

6.13 Cuando un *riesgo de corrupción* se materializa, el responsable de proceso debe: (i) informar a las autoridades la ocurrencia de los hechos, (ii) revisar el mapa de riesgos de corrupción, (iii) verificar si se tomaron acciones, y (iv)realizar monitoreo permanente. Con relación a la materialización de los *otros tipos de riesgo*, es necesario que el proceso tenga definida una acción de contingencia para implementar en caso de que se materialice, además debe verificar su mapa de riesgos y actualizar lo que considere necesario.

6.14 Los niveles de responsabilidad y autoridad de los servidores de la Entidad frente a los riesgos están establecidos en las líneas de defensa que se encuentran detalladas en la etapa de *monitoreo y revisión* de la presente guía.

6.15 El monitoreo y seguimiento a la gestión de los riesgos residuales identificados mediante la presente metodología, se realizará cuatrimestralmente por parte de la Dirección de Planeación y la Oficina de Control Interno, respectivamente, por lo cual los procesos deben realizar su reporte los primeros cinco (5) días hábiles del siguiente mes después del corte.

6.16 La Personería de Bogotá, D. C. ha dispuesto dos (2) documentos en Excel como herramientas para la identificación, análisis, valoración, evaluación, monitoreo y control de los riesgos de corrupción, estratégicos, de gestión, y de seguridad de la información.

7. CONDICIONES GENERALES

La Gestión del Riesgo en la Personería de Bogotá, D. C. inicia con el establecimiento de la Política de Administración del Riesgo por parte de la Alta Dirección, quien se compromete a proporcionar el Talento Humano y los recursos presupuestales y tecnológicos que permitan realizar una adecuada gestión del riesgo, promoviendo el cumplimiento de la misión, visión y objetivos institucionales.

La presente guía se desarrolla en dos etapas, *la primera* corresponde a la **metodología de Administración del Riesgo** y el paso a paso para la identificación, valoración, análisis, evaluación de controles, diseño de tratamiento, monitoreo y control de los riesgos con base en los lineamientos del Departamento Administrativo

de la Función Pública, contemplados en la Guía para la administración del riesgo y diseño de controles en Entidades públicas, versión 5.

Por su parte, *la segunda* etapa corresponde a las **herramientas** dispuestas por la Entidad para el registro de los riesgos y la creación del **Mapa de Riesgos Institucional** para su respectivo monitoreo y seguimiento por parte de las líneas de defensa, según los roles establecidos.

Las etapas antes mencionadas, se desarrollan en los numerales **8** y **9** del presente documento.

8. METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO EN LA PERSONERÍA DE BOGOTÁ, D. C.

Con el fin de garantizar una adecuada gestión del riesgo, que contribuya al cumplimiento de la misión, visión y objetivos de la Entidad, es necesario trabajar de manera articulada con todos los **responsables operativos** del proceso definidos en la caracterización de este, con integrantes del equipo de trabajo, así como con los **responsables de cada proceso**.

Desde el enfoque basado en riesgos, a continuación, se presenta la metodología general para la administración del riesgo en la Personería de Bogotá, D. C., la cual contiene directrices para cada una de las siguientes fases:

1. Identificación y descripción del Riesgo: comprende el análisis del contexto estratégico de la entidad, la caracterización de cada proceso y sus objetivos, así como el análisis frente a factores internos y externos, y la descripción del riesgo incluyendo su tipología.

2. Valoración del Riesgo: en esta fase, se *analiza* la probabilidad de ocurrencia del riesgo y su impacto previo a controles para determinar su *zona de riesgo inherente* o inicial; de igual manera, se *evalúa* la efectividad de los controles para determinar la *zona de riesgo residual* a partir de la cual se establecerá un tratamiento para su posterior monitoreo y control.

3. Tratamiento del Riesgo: con base en la identificación de la zona de riesgo residual, en esta fase, el proceso establece *estrategias que permitan combatir el riesgo*; a partir de lineamientos establecidos toma la decisión de evitarlos, *reducirlos, transferirlos o aceptarlos.*

4. Monitoreo y Revisión: el seguimiento a los controles y acciones de tratamiento definidas en la fase anterior, se realiza a través de una *Línea Estratégica* y tres *Líneas de Defensa* que involucran a todos los servidores de la Entidad. En esta fase, también se relacionan las acciones a ejecutar en caso de materializarse algún riesgo.

8.1 IDENTIFICACIÓN Y DESCRIPCIÓN DEL RIESGO

La etapa de identificación de los riesgos se debe realizar con base en el contexto estratégico de la Entidad, en la caracterización de cada proceso y en factores internos y externos que puedan afectar el cumplimiento de los objetivos estratégicos y de proceso planeados.

Esta etapa está compuesta por los siguientes aspectos:

- ✓ Análisis del contexto
- ✓ Etapas para la identificación de riesgos
- ✓ Tipos de Riesgo
- ✓ Descripción y/o estructura de riesgos
- ✓ Clasificación del Riesgo

8.1.1 Análisis del contexto

El contexto se entiende como las condiciones internas y externas, que pueden generar eventos que afectan negativa o positivamente el cumplimiento de la misión y objetivos de la Entidad, dentro de esta etapa se analizan los objetivos estratégicos y los objetivos de proceso, lo cuales deben ser específicos, medibles, alcanzables, relevantes y temporales.

Para el caso del *contexto estratégico* en el que opera la Entidad, se debe realizar lo siguiente:

- Revisar la Misión y Visión de la Entidad
- Analizar si los Objetivos Estratégicos se encuentran alineados con la misión y visión institucional, así como su adecuada formulación y su desdoble hacia los objetivos de los procesos
- Identificar “Factores Claves de Éxito” de la Entidad

- Analizar debilidades, oportunidades, fortalezas y amenazas –DOFA- de la Entidad

Con relación al *contexto del proceso*, basados en su caracterización, se analiza lo mencionado a continuación:

- Objetivo(s) del proceso
- Alineación de los objetivos del proceso, con los objetivos estratégicos de la Entidad
- Alcance
- Actividades del proceso
- Procedimientos asociados
- Interrelación con otros procesos
- Responsables del proceso
- Puntos de riesgo del proceso
- Debilidades, oportunidades, fortalezas y amenazas del proceso

8.1.2 Etapas para la identificación de Riesgos

Partiendo del análisis del contexto interno y externo de la entidad y el del proceso, se *identifican los riesgos* para la consecución de sus objetivos en todos los niveles y se analizan como base para determinar cómo deben gestionarse.

En esta fase se deben determinar los eventos de riesgo, sus **causas** y sus **consecuencias**, para los cuales se requiere un **análisis detallado y exhaustivo**, dado que a partir de las causas y consecuencias se definen los controles y acciones de tratamiento para los riesgos identificados.

De igual forma, en la identificación de riesgos, se busca conocer los eventos potenciales, estén o no bajo el control de la Entidad, que ponen en riesgo el logro de su misión, funciones y objetivos.

El punto de partida para la identificación del riesgo debe ser información histórica (interna o de entidades similares) y discusiones con las partes involucradas acerca de aspectos históricos, actuales o en desarrollo; para este análisis se puede considerar la siguiente información:

- Experiencia local
- Entrevistas estructuradas

- Planes estratégicos
- Informes posteriores a los eventos
- Experiencia organizacional pasada
- Resultados de informes de auditorías, seguimientos y visitas en sitio.
- Bases de datos de incidentes, de riesgos anteriores, entre otros.

Por otro lado, además de la información anterior, cada proceso puede revisar los siguientes *factores*, con el fin de identificar la presencia de otros riesgos u oportunidades:

- Salidas no conformes
- PQRSDF
- Planes de mejoramiento
- Auditorías
- Informes de gestión
- Informes de control interno
- Plan anticorrupción y de atención al ciudadano y sus seguimientos
- Eventos relacionados con errores en las actividades realizadas por los servidores de la entidad, que pueden originarse por ausencia de capacitaciones
- Eventos relacionados con la infraestructura tecnológica y física como daño en equipos, caída de redes, aplicaciones, o derrumbes, inundaciones, incendio, entre otros

Finalmente, en el proceso de identificación de los riesgos, también se debe considerar un análisis general del posible impacto económico y/o reputacional al cual se expone la Entidad en caso de materializarse algún riesgo. DAFP (2020)

8.1.3 Tipos de Riesgo

Una vez identificados los riesgos y realizado un análisis general de sus posibles consecuencias, se establece el tipo de riesgo. En la presente metodología, los tipos de riesgo a identificar y gestionar son:

- Riesgos Estratégicos
- Riesgos de Gestión
- Riesgos de Corrupción
- Riesgos de Seguridad de la Información

Por otra parte, en razón a que la administración de los riesgos *ambientales*, de *seguridad y salud en el trabajo* y de *contratación* de bienes y servicios no se encuentra contemplada en la presente metodología; se aclara que serán gestionados de conformidad con los lineamientos legales vigentes aplicables, de la siguiente manera:

- Riesgos ambientales: De conformidad con los lineamientos de la Secretaría Distrital de Ambiente, el Programa Institucional de Gestión Ambiental - PIGA y el Sistema de Gestión Ambiental de la Personería de Bogotá, D. C.

- Riesgos de seguridad y salud en el trabajo: De conformidad con los lineamientos del Ministerio de Trabajo Ley 1562 de 2012, Decreto 052 de 2017 y el Sistema de Gestión de Seguridad y Salud en el Trabajo –SG SST.

- Riesgos de contratación de bienes y servicios: De conformidad con los lineamientos de la Agencia Nacional de Contratación- Colombia Compra Eficiente.

A continuación, se describen uno a uno los riesgos a gestionar mediante la presente Guía de Administración del Riesgo y la manera de identificarlos:

Riesgos estratégicos: Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la Entidad.	**Riesgos de Gestión:** Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos de la Entidad, en la presente metodología el riesgo de Gestión contiene los riesgos que se pueden clasificar como operativo, tecnológico, financiero, de imagen o reputacional.
Riesgos de Seguridad de la Información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).	**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

8.1.3.1 Riesgos Estratégicos:

La identificación de posibles eventos de riesgo estratégico se realiza por parte de cada proceso, con la participación del responsable de proceso, el referente de gestión y su equipo de trabajo, con base en el análisis del contexto definido en el

numeral 8.1.1 y los parámetros del numeral 8.1.2, a partir del cumplimiento del **objetivo estratégico** al cual contribuye.

Este análisis constituye el insumo para la administración de los riesgos estratégicos y su consolidación en el mapa de riesgos institucionales, debe ser actualizado al menos una vez al año.

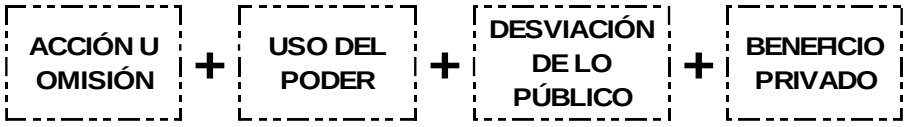
Nota: Si al realizar este ejercicio se determina la existencia de una *oportunidad*, esta deberá ser gestionada de conformidad con la metodología definida por la Entidad.

8.1.3.2 Riesgos de Gestión:

La identificación de posibles eventos de riesgos de gestión debe ser realizada por el responsable de proceso, con el apoyo del referente de gestión y su equipo de trabajo, quienes deben ser conocedores de las acciones ejecutadas desde el proceso. Esta identificación se realiza en primer lugar con base en las actividades establecidas en la **caracterización del proceso** y, teniendo en cuenta el contexto definido en el numeral 8.1.1 y los parámetros del numeral 8.1.2.

8.1.3.3 Riesgos de Corrupción:

La identificación de los riesgos de corrupción se realiza con base en las actividades desarrolladas por los procesos y es definida como la "*posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado*", en razón a esto, para que un riesgo de corrupción sea considerado como tal, en el mismo evento de riesgo deben concurrir TODOS los componentes mencionados a continuación, de lo contrario podría tratarse de otro tipo de riesgo.



Nota: el riesgo de corrupción debe estar descrito de manera clara y precisa, su redacción no debe dar lugar a ambigüedades o confusiones, además, su descripción debe contener los cuatro componentes antes mencionados. DAFP (2020).

Por otro lado, en la etapa de identificación de los riesgos de corrupción, cada proceso debe identificar posibles eventos relacionados con **riesgos de soborno** en la Entidad. El soborno es definido como[5]:

a) La promesa, el ofrecimiento o la concesión a un funcionario público, en forma directa o indirecta, de un beneficio indebido que redunde en su propio provecho o en el de otra persona o entidad con el fin de que dicho funcionario actúe o se abstenga de actuar en el cumplimiento de sus funciones oficiales;

b) La solicitud o aceptación por un funcionario público, en forma directa o indirecta, de un beneficio indebido que redunde en su propio provecho o en el de otra persona o entidad con el fin de que dicho funcionario actúe o se abstenga de actuar en el cumplimiento de sus funciones oficiales (Ley 970, 2005, art. 15).

Teniendo en cuenta lo anterior, y de conformidad con la Ley 412 de 1997, mediante la cual el Gobierno Nacional aprobó la "*Convención Interamericana contra la Corrupción"* y la Ley 970 de 2005 en la cual fue aprobada la "*Convención de las Naciones Unidas contra la Corrupción*"; la Veeduría Distrital, *como parte de sus funciones de apoyo en la prevención de la corrupción en las entidades y organismos públicos*, elaboró la **Metodología de prevención de Riesgos de Soborno en Entidades Públicas,** que busca "*implementar medidas de prevención de riesgos de soborno en las entidades públicas*"[6] a través de los siguientes pasos:

1. Identificación de señales de alerta
2. Identificación de procesos a analizar
3. Conocer el proceso
4. Identificación de puntos críticos
5. Sistematización de información
6. Análisis de Riesgo
7. Adopte medidas de control interno
8. Formulación de una política antisoborno
9. Socialización interna y externa

Nota: como parte de la etapa de identificación de riesgos de corrupción, los procesos en los que se pueda presentar un posible evento de soborno en las actividades que realiza, deben analizar este tipo de riesgo, siguiendo los lineamientos de la Metodología establecida por la Veeduría Distrital.

[5] Convención de las Naciones Unidas contra la Corrupción, adoptada por la Asamblea General de las Naciones Unidas, en Nueva York, el 31 de octubre de 2003.

[6] Metodología prevención de Riesgos de Soborno en entidades públicas. Veeduría Distrital, 2019

Finalmente, es de mencionar que la Personería de Bogotá, D. C. adoptó su **Código de Integridad** mediante la Resolución 1289 de 2018, fundamentado en los valores de honestidad, respeto, compromiso, diligencia, justicia, crecimiento personal y liderazgo. Este código, junto con el Plan de gestión de integridad que se define cada año por parte de la Dirección de Talento Humano, operan como *controles institucionales para los riesgos de corrupción*, dado que, su aplicación busca mitigar directamente el riesgo de soborno y otras actuaciones relacionadas con corrupción al interior de los procesos de la entidad.

Por lo anterior, para la gestión de los riesgos de corrupción se deben vincular a los gestores de integridad de cada proceso, y promover el conocimiento y aplicación del Código de integridad como control, sin perjuicio de los demás controles que se definan al interior del proceso.

8.1.3.4 Riesgos de Seguridad de la Información:

Considerando los riesgos de seguridad de la información como “pérdida o daño de un activo de información”, para determinar los riesgos de este tipo, se debe realizar en primer lugar, un inventario de **activos de información del proceso**, de conformidad con el formato establecido en la Entidad para tal fin. Entre los activos de información se pueden encontrar los siguientes:

- Aplicaciones de la entidad
- Servicios web
- Redes
- Información física o digital
- Tecnologías de información TI

Para identificar los activos, se debe: (i) listar los activos por cada proceso, (ii) identificar el dueño de los activos, (iii) clasificar los activos, (iv) clasificar la información, (v), determinar la criticidad del activo, y (6) identificar si existe infraestructura crítica. No obstante, con el fin de profundizar en la etapa de identificación de activos de la información, se requiere verificar el Modelo Nacional de Gestión de Riesgo de Seguridad de la información en Entidades Públicas.

A través de la identificación de activos, se busca que la Entidad determine cuál es su activo de información más importante que tiene, bien sea bases de datos, archivo, servidores web, entre otros; una vez identificado su nivel de importancia la entidad puede determinar qué es lo que más debe proteger para garantizar la prestación del servicio y su funcionamiento interno y de cara al ciudadano.

Una vez realizado el inventario de activos de la información, se procede a la identificación de los Riesgos de Seguridad de la Información, los cuales están basados en la violación o afectación de la confidencialidad, integridad o disponibilidad de la información y se hallan a partir de los activos de información previamente identificados.

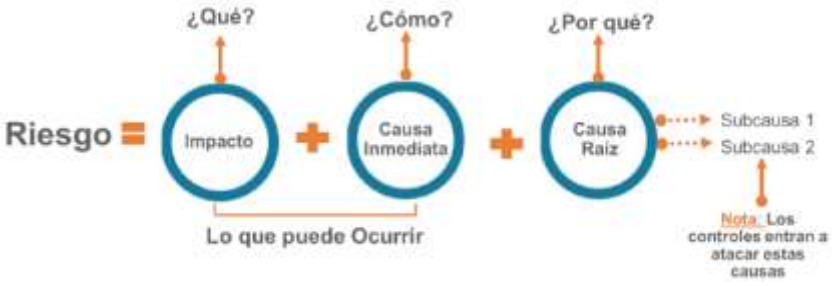
Con el fin de garantizar la correcta *identificación de los riesgos de seguridad de la información*, remitirse al Anexo 2 "*Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas*", de la Guía para la Administración *del riesgo y el diseño de controles en entidades públicas*, del Departamento Administrativo de la Función Pública- DAFP (2020).

Nota: la Dirección de Tecnologías de la información y las comunicaciones de la Entidad acompañará a los procesos en ésta y las siguientes etapas para la gestión de los riesgos de seguridad de la información, por medio de los profesionales designados.

8.1.4 Descripción y/o estructura de Riesgos

Una vez analizados los factores mencionados anteriormente, e identificados los riesgos que se pueden presentar en la organización, se procede a describir el riesgo, el cual debe ser definido de manera clara y debe contener detalles que sean de fácil entendimiento para todas las personas que lo lean.

Con el fin de facilitar la redacción del riesgo y el entendimiento universal de éste, el Departamento Administrativo de la Función Pública, a través de su Guía para la administración del riesgo y el diseño de controles en Entidades Pública, versión 5, ha propuesto la siguiente estructura:



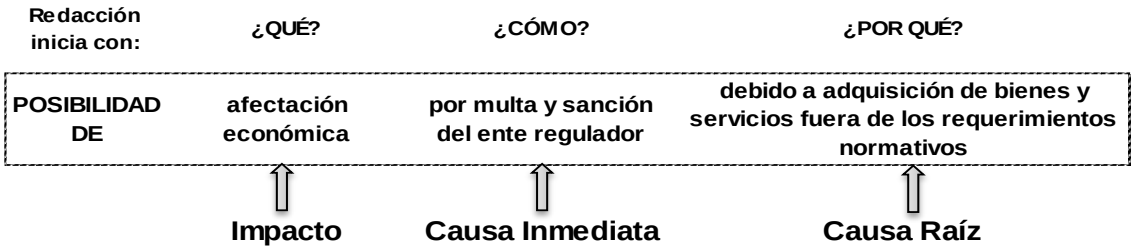
Definiendo uno a uno los aspectos de la estructura, encuentra lo siguiente:

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

- *Causa inmediata:* circunstancias evidentes sobre las cuales se presenta el riesgo, sin embargo, no constituye la causa principal del riesgo.

- *Causa Raíz:* es la causa principal, corresponde a las razones por las cuáles se puede presentar el riesgo, con base en las cuales se definen los controles.

Una vez identificados el impacto, la causa inmediata y la causa raíz, se procede a la redacción del riesgo, la cual podría iniciar con la frase "**Posibilidad de**", quedando de la siguiente manera, según el ejemplo propuesto por el DAFP:



Por otra parte, a continuación, se relacionan algunas ***premisas*** para una adecuada redacción del riesgo: [7]

- No describir como riesgos omisiones ni desviaciones del control. *Ej. Errores en la liquidación de la nómina por fallas en los procedimientos existentes.*
- No describir causas como riesgos. *Ej. Inadecuado funcionamiento de la plataforma estratégica donde se realiza el seguimiento a la planeación.*
- No describir riesgos como la negación de un control. *Ej. Retrasos en la prestación del servicio por no contar con digiturno para la atención.*
- No existen riesgos transversales, lo que pueden existir son causas transversales. *Ej. Pérdida de expedientes.*

8.1.5 Clasificación del Riesgo

De igual manera, los riesgos se pueden agrupar en las siguientes categorías que deben ser tenidas en cuenta en el proceso de identificación de los riesgos estratégicos, de gestión y de seguridad de la información:

[7] Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5. DAFP, 2020.

Categoría de riesgo	Definición
Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fallas tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

8.2 VALORACIÓN DEL RIESGO

La valoración del riesgo consiste en determinar la probabilidad de ocurrencia del riesgo y el nivel de impacto en caso de su materialización, esta fase aplica para todos los riesgos identificados y busca hallar las Zonas de Riesgo *Inherente* y *Residual*, a través de los siguientes elementos:

- ✓ Análisis de Riesgos
- ✓ Evaluación de Riesgos

8.2.1 Análisis de Riesgos

En el análisis de riesgo se busca establecer la probabilidad de ocurrencia de éste y su impacto, con el fin de identificar la **Zona de Riesgo Inherente o inicial**, es decir antes de los controles. Este análisis está compuesto por tres componentes:

- Determinar la probabilidad
- Determinar el impacto
- Determinar la zona de riesgo inherente

8.2.1.1 Determinar la probabilidad:

Para determinar la probabilidad de ocurrencia de los riesgos estratégicos, *de gestión y de seguridad de la información*, se analiza la exposición al riesgo, es decir, se debe identificar el número de veces que se ejecuta la actividad generadora del riesgo en el término de un año, o el número de veces que pasa por el punto de riesgo en este mismo periodo, de acuerdo con lo establecido en la siguiente tabla:

Tabla 1. Ponderación de la probabilidad para riesgos Estratégicos, de Gestión y de Seguridad de la Información

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5. DAFP, 2020.

Por otro lado, para determinar la probabilidad de ocurrencia de los *Riesgos de Corrupción*, se analiza qué tan posible es que ocurra el evento de riesgo frente a hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo y se analiza el número de eventos en un periodo determinado. Si no se cuenta con datos históricos, se hará de acuerdo con la experiencia de los responsables que desarrollan el proceso y de sus factores internos y externos.

En caso de un hecho que no se ha presentado, pero es posible que suceda, se analiza la presencia de factores internos y externos que pueden propiciar el riesgo.

Tabla 2. Ponderación de la probabilidad de Riesgos de Corrupción

Nivel	Probabilidad	Frecuencia de los eventos
1	Rara vez	No se tiene conocimiento de eventos similares en la entidad en los últimos 5 años
2	Improbable	Eventos similares ocurrieron al menos una vez en los últimos 5 años
3	Posible	Se tiene conocimiento de la ocurrencia de eventos similares al menos una vez en los últimos 2 años
4	Probable	Eventos similares se han presentado en la entidad al menos una vez en el último año
5	Casi seguro	Eventos similares se han dado más de una vez en la entidad en el último año

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 4. DAFP, 2018.

No obstante lo anterior, aplicará un mismo mapa de calor para los riesgos estratégicos, de gestión, de seguridad de la información, así como los de corrupción.

8.2.1.2 Determinar el impacto:

Para determinar el impacto originado a partir de la materialización del evento, se utiliza la siguiente tabla de criterios para los *riesgos estratégicos, de gestión y de seguridad de la información*, de conformidad con la versión 5 de la Guía para la administración del riesgo y diseño de controles en entidades públicas del DAFP (2020); las variables principales de estos criterios son los **impactos económicos** y **reputacionales**, que agrupan afectaciones a la ejecución presupuestal, pagos por sanciones económicas, indemnizaciones a terceros, sanciones por incumplimientos de tipo legal, y afectación a la imagen institucional por vulneraciones a la información o fallas en la prestación del servicio.

Tabla 3. Criterios para definir el área de Impacto en Riesgos Estratégicos, de Gestión y de Seguridad de la Información

	Afectación Económica (o presupuestal)	Pérdida Reputacional
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de alguna área de la organización
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta dircetiva y accionistas y/o de provedores
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitarios sostenible a nivel país

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5. DAFP, 2020.

Nota: En caso de que el impacto sea calificado con criterios de afectación económica y reputacional, se debe elegir el nivel más alto para determinar el impacto del evento, el cual contribuirá a la definición de la zona de riesgo inherente.

Por otro lado, para el análisis de impacto de los *riesgos de corrupción*, el Departamento Administrativo de la Función Pública a través de la versión 4 de la Guía de administración del riesgo y diseño de controles (2018), definió un cuestionario para calificar el impacto, y determinar el área de impacto. Este cuestionario se encuentra en el formato del Mapa de Riesgos de corrupción de la Entidad, y se debe responder Sí o No a cada una de las preguntas marcando con una X en la opción que corresponda, al finalizar el cuestionario el nivel de impacto aparecerá automáticamente en la celda definida para ello.

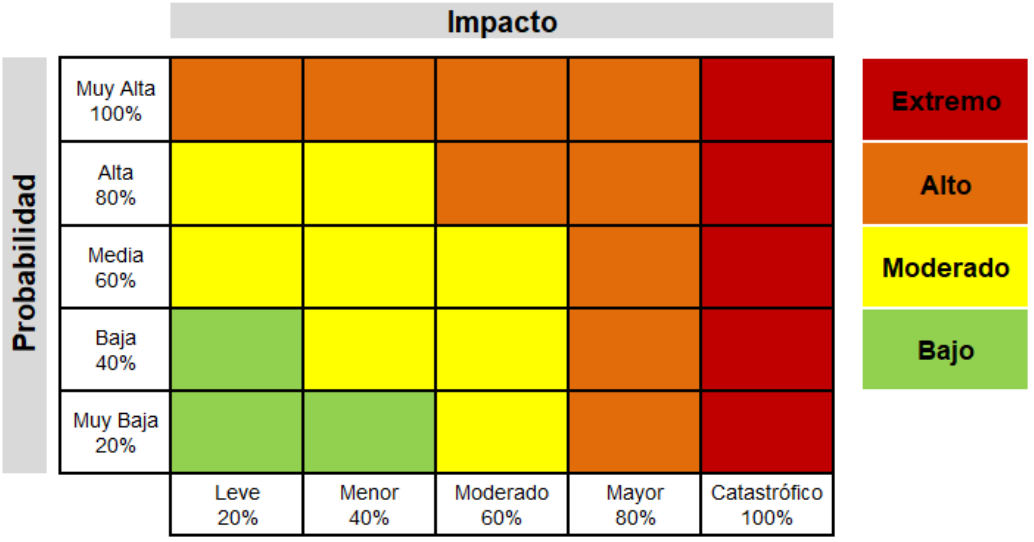
Nota: El *impacto* para los *riesgos de corrupción* siempre debe estar ubicado en las columnas "moderado", "mayor" y "catastrófico", dado que sus consecuencias siempre serán significativas; por lo cual para esta clase de riesgos no aplican los niveles de impacto insignificante y menor.

8.2.1.3 Determinar la Zona de Riesgo Inherente:

Una vez analizada la probabilidad de ocurrencia y el impacto del riesgo, se procede a determinar la *Zona de Riesgo Inherente*, conocida como zona de riesgo inicial o antes de controles.

Para determinar los *niveles de severidad* o la *zona de riesgo* de acuerdo con el siguiente Mapa de Calor, se debe realizar la combinación entre la probabilidad y el impacto determinados en las dos etapas precedentes. La zona de riesgo será el punto de convergencia entre estos dos aspectos, y puede estar en un nivel Extremo, Alto, Moderado o Bajo como se muestra a continuación:

Imagen 1. Mapa de Calor



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5. DAFP, 2020.

Nota: los riesgos de corrupción, solamente pueden estar ubicados en las Zonas de Riesgo *moderada*, *alta* y *extrema* dentro del mapa de calor.

8.2.2 Evaluación de Riesgos

La etapa de evaluación de riesgos consiste en determinar la **Zona de Riesgo Residual**, es decir, la zona de riesgo después de evaluar controles; se busca confrontar los resultados de la etapa de análisis de riesgo (inherente), frente a los *controles* establecidos para cada riesgo. Los pasos por seguir en esta etapa son:

- Identificación y diseño de controles
- Análisis y evaluación de controles
- Determinar la Zona de Riesgo Residual

8.2.2.1 Identificación y diseño de controles:

Para realizar una adecuada evaluación de los controles definidos en cada riesgo e identificar si éstos son adecuados para evitar que se genere algún evento que ponga en riesgo el cumplimiento de los objetivos institucionales, es necesario analizar los criterios mínimos que debe contener cada control con el fin de garantizar su efectividad. A continuación, se describen las consideraciones a tener en cuenta en la *estructura* para la descripción de los controles: [8]

- *Responsable de ejecutar el control:* se debe identificar el cargo de quien realizará el control o el sistema que lo ejecuta, si es de tipo automático.

- *Acción:* se describe mediante un verbo la acción a ejecutar como parte del control.

- *Complemento:* se registran los detalles que permitan identificar el objeto del control.

De otra parte, en la estructuración y diseño de los controles también se deben tener en cuenta los *tipos de controles* existentes los cuales servirán como parte de los

[8] Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5. DAFP, 2020.

atributos para evaluar los controles de cada riesgo. Entre los tipos de control encontramos lo siguientes:

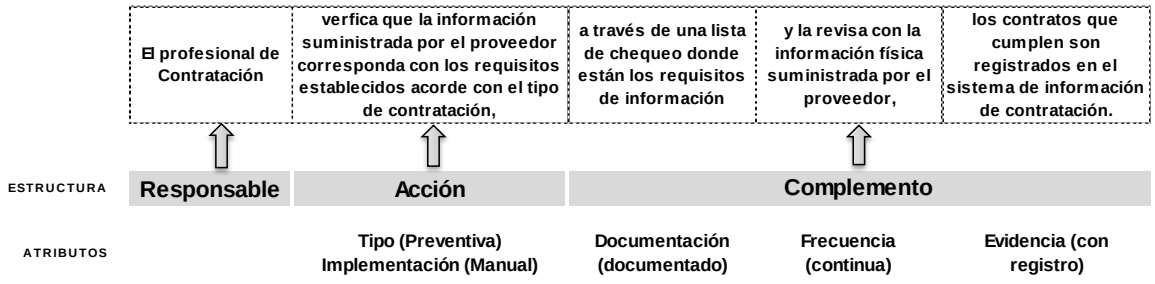
- *Preventivos:* control accionado en la *entrada* del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado. Va a las causas del riesgo, atacan la probabilidad de ocurrencia del riesgo.

- *Detectivos:* control accionado durante la *ejecución* del proceso. Estos controles detectan el riesgo, pero generan reprocesos. Detecta que algo ocurre y devuelve el proceso a los controles preventivos, atacan la probabilidad de ocurrencia del riesgo.

- *Correctivos:* control accionado en la *salida* del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos. Atacan el impacto frente a la materialización del riesgo.

Finalmente, se debe analizar la forma en la cual se implementará el control, si será automática o manual, así como determinar si se documentarán las acciones de control, cuál será su frecuencia y si se dejará registro o no de las actividades realizadas.

Con base en lo anterior, y teniendo en cuenta las características que debe contener un control para evitar o reducir la generación de un evento de riesgo, se presenta el siguiente ejemplo propuesto por el DAFP, en el cual se puede identificar la estructura y los atributos base para la identificación y posterior calificación del control en los Riesgos Estratégicos, de Gestión y de Seguridad de la Información:



8.2.2.2 Análisis y evaluación de controles:

Una vez analizadas las consideraciones a tener en cuenta al momento de diseñar un control que garantice la mitigación de los riesgos, se presenta en la siguiente matriz la calificación que se otorga a cada atributo, y con base en la cual se identifica la efectividad del control para determinar la *Zona de Riesgo Residual de los riesgos estratégicos, de gestión y de seguridad de la información,* a partir de la cual se tomará la decisión de establecer acciones de tratamiento o no, de conformidad con los aspectos de tratamiento definidos para cada zona.

Tabla 4 Atributos para la evaluación del control en los Riesgos Estratégicos, de Gestión y de Seguridad de la Información

Características			Descripción	Peso
Atributos de Eficiencia	**Tipo**	**Preventivo**	Va hacia las causas del riesgo, aseguran el resultado final esperado. **(Afecta probabilidad)**	**25%**
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos. **(Afecta probabilidad)**	**15%**
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación. **(Afecta impacto)**	**10%**
	Implementación	**Automático**	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	**25%**
		Manual	Controles que son ejecutados por una persona., tiene implícito el error humano.	**15%**
Atributos de Formalización	**Documentación**	**Documentado**	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
		Sin Documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso	-

	Frecuencia	**Continua**	Este atributo identifica a los controles que se ejecutan siempre que se realiza la actividad originadora del riesgo.	-
		Aleatoria	Este atributo identifica a los controles que no siempre se ejecutan cuando se realiza la actividad originadora del riesgo	-
	Evidencia	**Con Registro**	El control deja un registro que permite evidenciar la ejecución del control	-
		Sin Registro	El control no deja registro de la ejecución del control	-

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5. DAFP, 2020.

Los *atributos de formalización* presentados en la tabla anterior, permiten conocer el entorno del control y complementar el análisis con elementos cualitativos, sin embargo, estos no tienen alguna incidencia directa en su efectividad. Mientras que los *atributos de eficiencia* permiten calificar la efectividad de los controles asociados a cada uno de los riesgos con el peso porcentual definido en la tabla anterior; con base en el resultado de esta calificación se hallará el nuevo nivel de probabilidad y de impacto que permitirán determinar la zona de riesgo residual.

Por su parte, es de aclarar que el diseño y evaluación de los controles asociados a los *Riesgos de Corrupción,* se seguirá realizando según lo estipulado en la Guía de administración del riesgo y diseño de controles, versión 4, DAFP (2018). El cuestionario para calificar los controles de este tipo de riesgos se encuentra parametrizado en el formato del Mapa de Riesgos de corrupción para su evaluación, el cual determina si los controles existentes son fuertes, moderados o débiles, e indica el número de *filas a movilizar en la probabilidad* y el número de *columnas a movilizar en el impacto* dentro del mapa de calor, únicamente en caso de que la calificación de los controles haya sido moderada o fuerte.

Pese a lo mencionado, es de recordar que para los riesgos de corrupción la *calificación del impacto* de la zona de riesgo residual (después de controles), debe ser la misma de la zona de riesgos inherente (inicial o antes de controles) pues las consecuencias negativas en caso de presentarse algún evento de corrupción, no se pueden minimizar en comparación con la definida inicialmente.

Tabla 5 Atributos para la evaluación del control en los Riesgos de Corrupción

Criterio de evaluación	Aspecto a evaluar en el diseño del control
1. Reponsable	¿Existe un responsable asignado a la ejecución del control?
	¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?
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?
	Controles que son ejecutados por una persona., tiene implícito el error humano.
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, Ej.: verificar, validar, cotejar, comparar, revisar, etc.?
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?
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?
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?

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 4. DAFP, 2018.

Es de señalar la importancia de mantener una adecuada implementación de cada uno de los controles que permita realizar una evaluación ajustada a la realidad, pues un óptimo análisis y evaluación de los controles permite detectar aspectos a mejorar tanto en su diseño como en su ejecución.

Nota: la *calificación* de los controles de los Riesgos Estratégicos, de Gestión y de Seguridad de la Información, se realiza con base en los atributos de la tabla No. 4. Cuando existe más de un control para un mismo riesgo, la *evaluación* de los controles se realiza de manera *acumulativa*, es decir el resultado de la calificación de la probabilidad y del impacto del primer control, se toma como base para la calificación del segundo control, el resultado de la calificación del segundo control es la base para la evaluación del tercer control y así sucesivamente. Por cada uno de los controles establecidos en un mismo riesgo, se deberán calificar los atributos tanto de eficiencia como los de carácter informativo. [9] La parametrización de esta calificación, se encuentra en el formato del Mapa de Riesgos de Gestión.

8.2.2.3 Identificación Zona de Riesgo Residual:

La Zona de Riesgo Residual, es la resultante del análisis de la zona de riesgo inherente frente a la evaluación de los controles, de acuerdo con la calificación de cada uno de los atributos tanto en riesgos estratégicos, de gestión, de seguridad de la información, y de corrupción, según las tablas No. 4 y 5, respectivamente.

[9] Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5. DAFP, 2020.

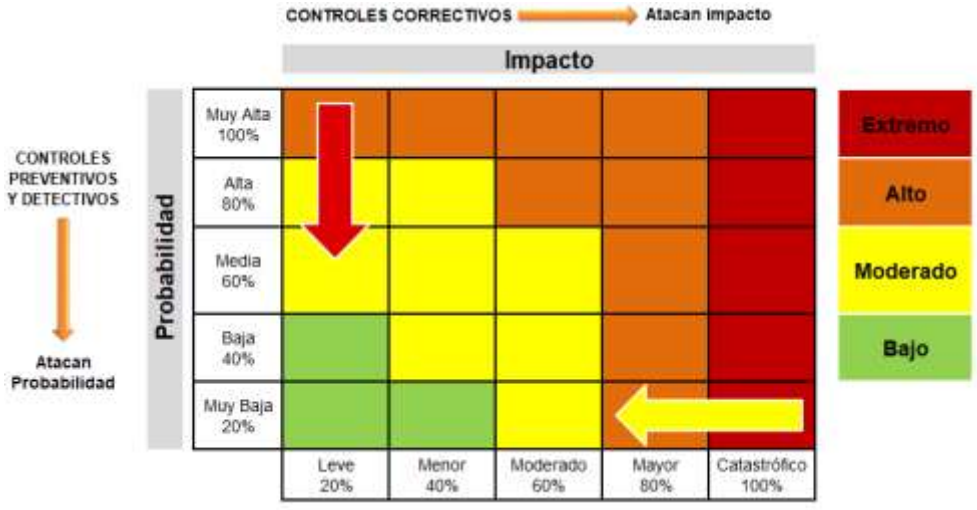
Para los riesgos estratégicos, de gestión y de seguridad de la información, realizada la evaluación de los controles y dependiendo el tipo de control aplicado (preventivo, detectivo o correctivo), se determina el movimiento a realizar en el eje de probabilidad y en el eje de impacto.

Por otro lado, el movimiento en el mapa de calor para los riesgos de corrupción, depende si la calificación de sus controles fue moderada o fuerte, basada en lo cual se identificará el número de *filas a desplazar en probabilidad*. Esto, teniendo en cuenta que para este tipo de riesgos el impacto no cambia con relación al establecido inicialmente, por lo cual no hay desplazamiento de columnas dentro del mapa de calor.

Es de precisar que, los **controles preventivos** y **detectivos** desplazan el grado de ***Probabilidad*** en el mapa de calor buscando siempre disminuir la probabilidad o probabilidades de que se presente el riesgo; mientras que los **controles correctivos** atacan el ***Impacto*** generado en caso de llegar a materializarse el riesgo, por lo cual, si los controles identificados en un riesgo no son de tipo correctivo no podrá desplazarse la columna impacto. Se aclara que, en razón a que los *riesgos de corrupción* no disminuyen su impacto en el mapa de calor, para estos riesgos no aplica el tipo de control correctivo.

A continuación, se presenta el movimiento a realizar en el mapa de calor una vez aplicados y evaluados los controles. En las flechas ubicadas dentro de la matriz, se puede observar el desplazamiento que ocurre dentro de ésta, indicando que para hallar la *probabilidad residual* se deben desplazar las filas hacia la parte inferior, y para determinar el *impacto residual* se desplazan las columnas hacia la izquierda:

Imagen 2. Movimiento en los ejes de probabilidad e impacto dentro del Mapa de Calor de acuerdo con el tipo de control aplicado

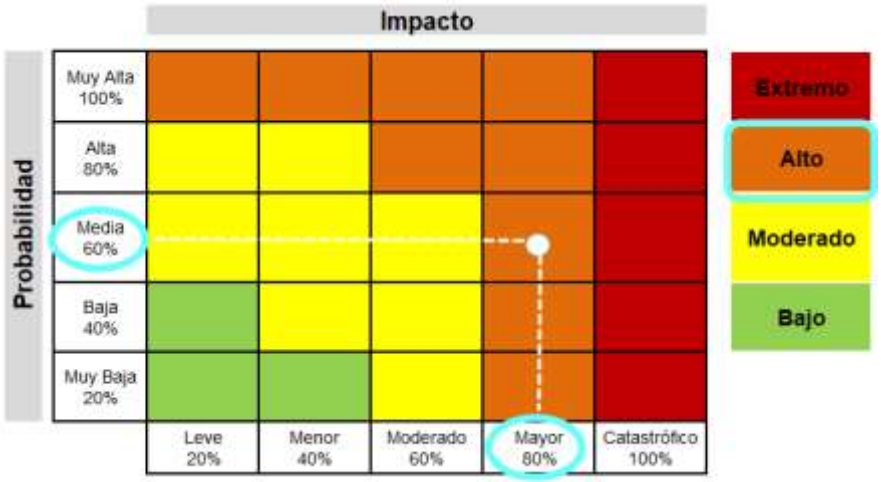


Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5. DAFP, 2020.

La cantidad de filas y/o columnas a movilizar depende del resultado arrojado en la evaluación de controles, para los *riesgos de corrupción* el formato de Mapa de Riesgos de corrupción indicará el número de filas a desplazar en probabilidad; mientras que, para los *riesgos estratégicos, de gestión y de seguridad de la información* el número de filas y columnas a desplazar dependen del porcentaje hallado en la evaluación de los controles a partir del cual se determinó la probabilidad y el impacto residuales.

Es decir, si por ejemplo se identificó que un riesgo tiene controles preventivos y correctivos, y *después de evaluados sus controles* el porcentaje de probabilidad residual hallado está entre el 41% y el 60% éste se ubicará en una probabilidad *media*, y si el porcentaje de impacto identificado se encuentra entre el 61% y el 80% se debe ubicar en la casilla de impacto *mayor*. Para este ejemplo, la *zona de riesgo residual* identificada sería "alta" pues es el punto de convergencia entre la probabilidad residual y el impacto residual. A continuación, se ilustra lo mencionado:

Imagen 3. Ejemplo Zona de Riesgo Residual



Fuente: Adaptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5. DAFP, 2020.

Realizado el movimiento en los ejes de probabilidad e impacto, según lo arrojado en la evaluación de los controles, se identifica la nueva zona de riesgo o la *Zona de Riesgo Residual* a partir de la cual se establecerá un tratamiento. Para los riesgos de corrupción, únicamente aplicaría Zonas de riesgo "moderada", "alta" y "extrema".

8.3 TRATAMIENTO DEL RIESGO

Finalizada la fase de valoración del riesgo, en la cual se identificó la Zona de Riesgo Residual, el responsable del proceso y su equipo de trabajo deben determinar las acciones adicionales a ejecutar o las estrategias que van a establecer para combatir ese riesgo.

El tratamiento del riesgo, es conocido como la respuesta establecida por la primera línea de defensa para la mitigación de los riesgos de su proceso, de acuerdo con el nivel de **Riesgo Residual** identificado. Para establecer el tratamiento, los dueños de los procesos deben tener en cuentan la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto de este y la relación costo-beneficio de las medidas de tratamiento.[10]

El tratamiento de los riesgos residuales, se enmarca en las siguientes categorías:

Tabla 6. Opciones de tratamiento riesgos residuales

Categoría de tratamiento	Definición
Evitar el Riesgo	Después de realizar un análisis y considerar que el nivel de riesgo es demasiado ALTO, se determina NO asumir la actividad que genera ese riesgo.
Reducir el Riesgo (mitigar)	Después de realizar un análisis y considerar los niveles de riesgo se implementan acciones que mitiguen el nivel de riesgo. Por lo general conlleva a la implementación de controles. (Plan de acción)
Transferir o compartir	Después de realizar un análisis se considera que la mejor estrategia es tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas. La responsabilidad económica reace sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputacional. **Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad.
Aceptar el Riesgo (asumir)	Después de realizar un análisis y considerar los niveles de riesgo se determina asumir el mismo conociendo los efectos de su posible materialización. Los riesgos se aceptan cuando la probabilidad es baja o muy baja y su impacto es leve o menor. **Ningún riesgo de corrupción podrá ser aceptado.

Teniendo en cuenta las opciones de tratamiento, la Personería de Bogotá, D. C. estableció los siguientes lineamientos que deben cumplir los líderes o responsables de proceso, según la Zona de Riesgo Residual en la cual se encuentre el riesgo:

[10] Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5. DAFP, 2020.

Tabla 7. Lineamientos para el tratamiento y monitoreo por Zona de Riesgo Residual

Zona de Riesgo	Opción de Tratamiento	Lineamientos para el tratamiento
Extremo Alto Moderado	**Reducir el Riesgo**	• Se deberá incluir el riesgo en el Mapa de Riesgos Institucional. • Se continuará con la ejecución de los controles existentes para este riesgo. • Se establecerán acciones preventivas y/o correctivas adicionales a los controles, que conlleven a **REDUCIR** la probabilidad de materialización y/o a disminuir su impacto, según el caso. • El monitoreo a estos riesgos por parte de la primera línea de defensa se hará con periodicidad **MENSUAL**, dejando evidencia de éste. • El seguimiento realizado por parte de la primera línea de defensa deberá ser registrado en el mapa de riesgos institucional y remitido a la Dirección de Planeación (segunda línea) con periodicidad **CUATRIMESTRAL**, durante los cinco primeros días del siguiente mes, dejando las evidencias correspondientes. • Si la primera línea de defensa determina que las acciones de tratamiento han sido efectivas, estas se implementarán como control.
Bajo	**Asumir el Riesgo**	• Se **ASUMIRÁ** el riesgo y se administrará por medio de las actividades propias del proceso asociado. • Se continuará con la ejecución de los controles existentes para este riesgo, por lo cual no se hace necesario establecer acciones adicionales. • El monitoreo a estos riesgos por parte de la primera línea de defensa se hará con periodicidad **CUATRIMESTRAL**, dejando evidencia de éste. • Cualquier modificación en la probabilidad o impacto de estos riesgos que cambie su Zona de Riesgo Residual, deberá ser actualizada y comunicada a la Dirección de Planeación, de conformidad con la presente tabla. **Nota:** ningún riesgo de corrupción puede ser aceptado o asumido.

Fuente: *elaboración propia con base en los lineamientos para tratamiento de riesgos en la Entidad.*

Para definir el *tratamiento del riesgo residual* se debe tener en cuenta:

- Cada proceso, antes del 15 de enero de cada vigencia, deberá enviar el Mapa de Riesgos del Proceso a la Dirección de Planeación para su revisión, consolidación y publicación, cuando aplique debe incluir plan de tratamiento.

- Para cada uno de los riesgos, y teniendo en cuenta el análisis de causas y la evaluación de controles, se definen *acciones de tratamiento*, se asignan los responsables de su ejecución y se determinan los recursos periodicidad, fecha de inicio y finalización, con el fin de con el fin de asegurar su implementación.

- En caso de encontrar que el tratamiento del riesgo requiere la participación de otro(s) proceso(s), el responsable del proceso deberá comunicar al (los) (las) responsables(es) de los procesos involucrados, con el fin de que se gestione el riesgo de forma concertada.

Una vez ejecutado el tratamiento, sus resultados deberán ser analizados por el proceso, de manera que se defina si a partir de ellos hay lugar a constituir un nuevo control (documentado), o a una mejora de un control existente.

Al finalizar la aplicación de la metodología general, el resultado de las diferentes etapas quedará consolidado en los formatos de Mapa Riesgos, de acuerdo con los lineamientos establecidos en la presente Guía.

8.4 MONITOREO Y REVISIÓN

En esta fase, se identificarán los *roles y responsabilidades* frente a la gestión del riesgo, de acuerdo con lo definido en la versión 4 del Manual operativo del MIPG, 2021. Igualmente, se determinarán las actividades a realizar en caso de que se *materialice* algún riesgo, en particular los riesgos de corrupción.

8.4.1 Roles y responsabilidades

Para la administración del riesgo en la Entidad y de conformidad con los lineamientos de la Séptima Dimensión del Modelo Integrado de Planeación y Gestión - MIPG, se han establecido unos roles y responsabilidades específicos para el monitoreo y seguimiento a las acciones implementadas para combatir el riesgo, organizados de la siguiente manera:

- Línea Estratégica
- Primera Línea de Defensa
- Segunda Línea de Defensa
- Tercera Línea de Defensa

A continuación, se describe la conformación de la línea estratégica y cada una de las líneas de defensa, y su rol frente a la administración del riesgo en la Entidad[11]:

8.4.1.1 Línea Estratégica:

Esta Línea analiza los riesgos y amenazas institucionales que puedan afectar el cumplimiento de los planes estratégicos, así como define el marco general para la gestión del riesgo (política de administración del riesgo) y garantiza el cumplimiento de los planes de la entidad. Su responsabilidad se centra en la emisión, revisión,

[11] Manual Operativo MIPG, versión 4. Departamento Administrativo de la Función Pública, 2021.

validación y supervisión del cumplimiento de políticas en materia de gestión del riesgo, seguimientos a la gestión, entre otros.

Líneas de Defensa	Responsables	Actividades frente a la Gestión del Riesgo
Línea Estratégica	Alta Dirección (Comité Institucional de Gestión y Desempeño) y Comité Institucional de Coordinación del Sistema de Control Interno	• Definición y evaluación de la Política de Administración del Riesgo y asegurarse de su permeabilización en todos los niveles de la Entidad. La evaluación debe considerar su aplicación en la entidad, cambios en el entorno que puedan definir ajustes, dificultades para su desarrollo y riesgos emergentes. • Monitoreo permanente de los riesgos de corrupción. • Monitoreo al estado de los riesgos aceptados, con el fin de identificar cambios sustantivos que afecten el funcionamiento de la entidad. • Revisar el 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. • Revisar los informes presentados de los eventos de riesgos materializados en la Entidad, incluyendo los riesgos de corrupción, las causas que dieron origen a los eventos de riesgos materializados. • Revisar las acciones correctivas establecidas para cada uno de los riesgos materializados, con el fin de revisar su eficacia para evitar en lo posible la repetición del evento.

8.4.1.2 <u>Primera Línea de Defensa:</u>

Su rol principal es el mantenimiento efectivo de controles internos, la ejecución de gestión de riesgos y controles en el día a día. Se encarga del mantenimiento efectivo de controles internos, por lo tanto, identifica, evalúa, controla y mitiga los riesgos.

Líneas de Defensa	Responsables	Actividades frente a la Gestión del Riesgo
Primera Línea de Defensa	Servidores en los diferentes niveles dentro de la organización, responsables o líderes de Procesos, Programas y Proyectos (realizan controles de gerencia operativa)	• Seguimiento a los indicadores de gestión de su proceso para asegurar su cumplimiento. • Coordinación con sus equipos de trabajo, de las acciones establecidas en la planeación institucional a fin de contar con información clave para el seguimiento o autoevaluación aplicada por parte de la 2ª línea de defensa. • Definición de objetivos con suficiente claridad para identificar y evaluar los riesgos. • Identificación y análisis de riesgos (analiza factores internos y externos; implica a los niveles apropiados de la dirección; determina cómo responder a los riesgos; determina la importancia de los riesgos). • La identificación de riesgos y el establecimiento de controles, así como su seguimiento, acorde con el diseño de dichos controles, evitando la materialización de los riesgos. • Monitoreo permanentemente a los cambios en el Direccionamiento Estratégico o en el entorno y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de sus procesos, para la actualización del mapa de riesgos de su proceso. • Revisión de las exposiciones al riesgo con los grupos de valor, proveedores, sectores económicos u otros (monitoreo del contexto estratégico). • Verificación de la adecuada identificación de los riesgos relacionados con fraude y corrupción. • Asegurar que el monitoreo a los riesgos se realiza acorde con la Política de Administración de riesgo establecida para la entidad.

Líneas de Defensa	Responsables	Actividades frente a la Gestión del Riesgo
Primera Línea de Defensa	Servidores en los diferentes niveles dentro de la organización, responsables o líderes de Procesos, Programas y Proyectos (realizan controles de gerencia operativa)	• Identificación, implementación y monitoreo a los controles con el apoyo de su equipo de trabajo. • Verificar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos. • Reporte a Planeación, de los eventos de riesgos que se han materializado en la Entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgos materializados, y aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas, a través del análisis de indicadores asociados a dichos objetivos; y establece un plan de acción para evitar que el evento se vuelva a presentar. • Revisa 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 de los objetivos.

8.4.1.3 <u>Segunda Línea de Defensa:</u>

Busca asegurar que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente. De igual manera, a través de actividades de control, esta Línea de Defensa supervisa y verifica la eficacia e implementación de las prácticas de gestión del riesgo, de tal forma que, como resultado de este seguimiento pueda orientar y generar alertas a la 1ª línea de defensa y a la Alta Dirección, cuando así lo considere.

Líneas de Defensa	Responsables	Actividades frente a la Gestión del Riesgo
Segunda Línea de Defensa	Jefes de la Dirección de Planeación, coordinadores de equipos de trabajo, coordinadores de sistemas de gestión, gerentes de riesgos (donde existan), líderes o coordinadores de contratación, financiera y de TIC, entre otros.	• Consolidación y análisis de información sobre temas claves para la entidad, base para la toma de decisiones y de las acciones preventivas necesarias para evitar materializaciones de riesgos. • Asesoría a la 1ª línea de defensa en temas clave para el Sistema de Control Interno, entre ellos los riesgos y sus controles. • Monitoreo a los cambios en el Direccionamiento Estratégico o en el entorno y cómo estos pueden generar nuevos riesgos o modificar los existentes en cada proceso, para la actualización del mapa de riesgos. • Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos, que han servido de base para llevar a cabo la identificación de los riesgos, y realiza las recomendaciones a que haya lugar. • Verificación, en el marco de la Política de Riesgos Institucional, que la identificación y valoración del riesgo de la primera línea sea adecuada frente al logro de objetivos y metas. • Verificación de la adecuada identificación de los riesgos relacionados con corrupción y evaluación de los mismos. • Aseguramiento de que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados frente a los riesgos identificados y funcionen correctamente, supervisan la implementación de prácticas de gestión de riesgo eficaces que garanticen la mitigación de una posible materialización. • Verificar que los responsables estén ejecutando los controles tal como han sido diseñados. • Asegurar que el monitoreo a los riesgos se realiza acorde con la Política de Administración de riesgo establecida para la entidad. • Seguimiento a las actividades de control establecidas para la mitigación de los riesgos de los procesos, a su documentación y actualización en los procedimientos. • Revisión de 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 que se vuelva a materializar el riesgo y lograr el cumplimiento a los objetivos.

8.4.1.4 <u>Tercera Línea de Defensa:</u>

Evalúa de manera independiente y objetiva los controles de la 2 ª línea de defensa con el fin de asegurar su efectividad y cobertura, igualmente, evalúa los controles de la 1ª línea de defensa.

Líneas de Defensa	Responsables	Actividades frente a la Gestión del Riesgo
Tercera Línea de Defensa	Oficina de Control Interno	• Asesoría, orientación técnica y recomendaciones frente a la administración del riesgo en coordinación con la Dirección de Planeación. • Monitoreo a la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo. • Brinda un nivel de asesoría proactiva y estratégica, frente a la Alta Dirección y los líderes de proceso. • Formación a la Alta Dirección y a todos los niveles de la entidad sobre las responsabilidades en materia de riesgos. • Evaluación de la efectividad de las acciones desarrolladas por la 2ª línea de defensa en aspectos como: cobertura de riesgos, cumplimientos de la planificación, mecanismos y herramientas aplicadas, entre otros, y genera observaciones y recomendaciones para la mejora. • Como resultado de la evaluación de la gestión del Riesgo comunica las deficiencias a la Alta Dirección y/o a las partes responsables para tomar las medidas correctivas, según corresponda. • Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos, que han servido de base para llevar a cabo la identificación de los riesgos, y realiza las recomendaciones a que haya lugar. • Seguimiento a las actividades de control establecidas para la mitigación de los riesgos de los procesos, su documentación y actualización en los procedimientos, y a la ejecución de los planes de acción establecidos como resultado de las auditorías realizadas, para cerrar las causas raíz del problema, evitando en lo posible la repetición de hallazgos o materialización de riesgos. • Asegurar que los controles sean efectivos, apunten al riesgo y estén funcionando de manera oportuna y efectiva. • Revisa el perfil de riesgo inherente y residual por cada proceso y consolidado y se pronuncia sobre cualquier riesgo que esté por fuera del perfil de riesgo de la Entidad, o cuya calificación de impacto o probabilidad del riesgo no sea coherente con los resultados de las auditorías realizadas.

8.4.2 Materialización de Riesgos

Cada proceso debe definir, por cada riesgo, una acción de contingencia a implementar en caso de que este se materialice, para ello deberá definir una estrategia apropiada, teniendo en cuenta las debilidades, oportunidades, fortalezas y amenazas del proceso, dejando registro y evidencia de ello.

En todo caso, una vez materializado el riesgo, el proceso debe revisar su mapa de riesgos con el fin de analizar cada una de las etapas de gestión del riesgo, y actualizar lo que sea pertinente. Para ello se podrá solicitar apoyo metodológico a la Dirección de Planeación y se le comunicará la versión actualizada de su Mapa de Riesgos, para su consolidación en el mapa institucional.

De otra parte, en caso de materializarse algún *riesgo de corrupción*, el responsable de proceso debe realizar los ajustes que considere pertinentes y adelantar las siguientes acciones:

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

9. HERRAMIENTAS PARA LA ADMINISTRACIÓN DEL RIESGO Y ELABORACIÓN DEL MAPA DE RIESGOS INSTITUCIONAL

Una vez identificados los riesgos estratégicos, de gestión, de corrupción y de seguridad de la información de conformidad con la metodología presentada en los numerales anteriores de esta Guía, se deben registrar en el formato Mapa de Riesgos de Corrupción y en la Plantilla Mapa de Riesgos Institucional, herramientas dispuestas por la Personería de Bogotá, D. C. para gestionar sus riesgos.

Al respecto, es de aclarar que, siguiendo los lineamientos del Departamento Administrativo de la Función Pública en la última versión de su Guía para la Administración del riesgo y el diseño de controles, se tomó la decisión de adaptar la "matriz mapa de riesgos" propuesta por la entidad en mención, con el fin de elaborar el mapa de riesgos estratégicos, de gestión y de seguridad de la información de la Personería de Bogotá, D. C., por lo cual éste no será un documento controlado y quedará como una plantilla anexa a la presente guía, denominada Mapa de Riesgos Institucional. Con relación a los riesgos de corrupción, y en razón a que se siguen identificando, valorando y evaluando con la metodología anterior, será usado el formato 01-FR-21 denominado Mapa de Riesgos de Corrupción, el cual se encuentra en los documentos controlados del Proceso de Direccionamiento Estratégico.

Las herramientas en mención, permiten registrar los riesgos y determinar su zona de riesgo inherente, así como realizar la evaluación de los controles existentes para identificar la zona de riesgo residual a partir de la cual se establecerá un plan de tratamiento para evitar la materialización de los riesgos identificados.

Finalmente, estas herramientas permiten a los líderes y referentes de proceso, registrar las acciones de tratamiento ejecutadas por cada uno de sus riesgos lo cual

contribuirá a la adecuada gestión del riesgo y al posterior monitoreo y seguimiento realizado por la segunda y tercera línea de defensa.

Con relación al formato ***01-FR-21*** donde se registrarán y gestionarán los Riesgos de Corrupción, a continuación, se especifican las secciones que contiene:

- **Hoja 1. Contexto**

Con base en los lineamientos del numeral 8.1.1 en esta hoja se identifica el contexto del proceso, se selecciona el proceso, se describen los riesgos del proceso y objetivo(s) estratégico(s) a los cuales apunta el proceso, las actividades del proceso y los factores internos y externos que afectan el proceso.

- **Hoja 2. Identificación**

En esta hoja se registran en la columna F los eventos de riesgos identificados, de igual manera se escriben las causas y consecuencias asociadas al riesgo y en la columna “I” se selecciona el tipo de riesgo en la lista que aparece en el formato.

- **Hojas 3 Probabilidad Riesgos**

Realizado el análisis de probabilidad para los riesgos corrupción según lo establecido en el numeral 8.2.1.1 de la presente guía, se selecciona de la lista desplegable que se encuentra en la columna “K” el nivel de probabilidad identificado por cada riesgo.

- **Hojas 4 Impacto Riesgos**

El nivel de impacto para los riesgos de corrupción, es generado de manera automática en la columna “C” de la hoja 4, como resultado de las respuestas a las preguntas de las columnas “G”, “M” y “S” de esta misma hoja.

- **Hoja 5. Zona de Riesgo Inherente**

La zona de riesgo inherente o inicial es el punto de convergencia entre la probabilidad y el impacto determinados en cada uno de los riesgos, y será generada automáticamente en la hoja 5 como resultado de la valoración realizada en pasos anteriores.

- **Hoja 6. Evaluación de controles**

De acuerdo con los atributos establecidos en el numeral 8.2.2.2, para la evaluación del diseño de controles de los riesgos de corrupción, se utilizarán los atributos de la hoja 6 donde se deben responder a cada una de las preguntas del cuestionario, seleccionando de la lista desplegable la respuesta que describa la situación real del control existente.

Con base en la información anterior, el formato arroja automáticamente la solidez del control. Esta información indica qué tan bien diseñado está el control existente y qué tan consistente es su ejecución

- **Hoja 7. Zona de Riesgo Residual**

Del resultado de la hoja 6 en la cual se evaluó el diseño de controles según atributos específicos, se halla en la hoja 7 la zona de riesgo residual o después de controles con base en la cual se determinará el tratamiento a implementar para mitigar el riesgo. En la columna “N” de esta misma hoja, se selecciona la opción de tratamiento de la lista desplegable atendiendo los lineamientos de la tabla 7 de la presente guía.

En esta hoja, en la columna “I” el formato indicará el número de filas a movilizar en probabilidad. Con base en este resultado, se elegirá de la lista desplegable de la columna “K” la probabilidad después de controles, que permitirá conocer de manera automática la zona de riesgo residual en la columna “M”.

En caso de que no haya lugar a desplazamientos, cuando las columnas “I” y “J” arrojen el número “0” o aparezcan en blanco, la zona de riesgo seguirá siendo la misma inicial o inherente. Tratándose de riesgos de corrupción, únicamente habrá disminución en la probabilidad, es decir, para el impacto no opera el desplazamiento, éste continuará siendo igual.

- **Hoja 8. Mapa de Riesgos**

Al finalizar la aplicación de la metodología general de acuerdo con los lineamientos establecidos en esta guía, el resultado de las diferentes etapas queda registrado en la hoja 8 Mapa de Riesgos del formato 01-FR-21, herramienta dispuesta por la Entidad para la administración de sus riesgos de corrupción.

Esta última hoja contiene de forma consolidada la información analizada y evaluada en cada una de las etapas de gestión del riesgo y por cada uno de los riesgos identificados. Además, se registra el plan de tratamiento para mitigar su

materialización, incluyendo las acciones a realizar, las fechas de ejecución, el indicador del riesgo y su fórmula, los recursos de los cuales se debe disponer y los responsables del cumplimiento de dichas acciones.

Es de aclarar, que dentro del formato en mención se encuentra el instructivo en cada una de las hojas para el diligenciamiento de las casillas.

Por otra parte, la plantilla en Excel mediante la cual se identificarán los riesgos estratégicos, de gestión y de seguridad de la información, conocida como ***Mapa de Riesgos Institucional***, está compuesta por las siguientes secciones:

- **Hoja 1. Instructivo**

En esta hoja se presenta el instructivo para el diligenciamiento de cada una de las casillas de la hoja 2 Mapa de Riesgos.

- **Hoja 2. Mapa de Riesgos**

En la hoja 2 *Mapa de Riesgos* se registra en la parte superior el nombre, objetivo y alcance del proceso, posteriormente, se selecciona el impacto según lo establecido en el numeral 8.2.1.2 de la presente guía y se describe la consecuencia, la causa inmediata, la causa raíz y se define el riesgo, así mismo, se selecciona el tipo de riesgo y su clasificación según lo indicado en el numeral 8.1.5, y se elige de la lista desplegable la probabilidad de acuerdo con los criterios del numeral 8.2.1.1. Por último, de las columnas “R” a la “Y” se evalúan los controles establecidos en cada uno de los riesgos, según los atributos de la tabla 4 de la presente guía.

Al diligenciar cada una de las columnas mencionadas anteriormente, el formato arroja de manera automática las zonas de riesgo inherente y residual; esta última zona se toma como base para determinar la necesidad de establecer un tratamiento, el cual se registrará de la columna “AF” a la columna “AK”.

De otra parte, en esta plantilla, se presenta, de la hoja 3 a la 7, la matriz de calor inherente y residual, y las tablas de probabilidad, impacto y valoración de controles, que sirven como orientación para el diligenciamiento de la hoja 2 Mapa de Riesgos.

Finalmente, a través de las herramientas del Mapa de Riesgos de Corrupción y Mapa de Riesgos Institucional mencionados en el presente numeral, se realiza monitoreo y control a las acciones de tratamiento establecidas por cada riesgo.

El monitoreo a los riesgos de corrupción será registrado por parte del *referente de gestión* del proceso, en las columnas “Y”, “Z” y “AA” de la hoja 8 del formato 01-FR-21; mientras que el monitoreo para los riesgos estratégicos, de gestión y de seguridad de la información, se registrará en las columnas “AL”, “AM” y “AN” de la hoja denominada mapa final, de la Plantilla Mapa de Riesgos Institucional que hace parte de los anexos de esta guía. El registro de estas actividades, se debe realizar cada cuatrimestre, de acuerdo con las indicaciones de la Dirección de Planeación, como Segunda Línea de Defensa.

10. ANEXOS

Anexo 1. Plantilla Mapa de Riesgos Institucional (riesgos estratégicos, de gestión y de seguridad de la información)