GUÍA DE ADMINISTRACIÓN DE RIESGOS

VERSIÓN 3

2025

ALCALDÍA DISTRITAL DE BARRANQUILLA

TABLA DE CONTENIDO

Índice de Tablas

Índice de Ilustraciones

1. PRESENTACIÓN

La Alcaldía Distrital de Barranquilla actualiza su Guía de Administración de Riesgos a la versión 3 con un enfoque de gobernanza de riesgos orientado a resultados, que privilegia la prevención, la toma de decisiones informada y la creación de valor público. Esta versión se articula con ISO 31000:2018, la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas del DAFP (v6) y el Marco Coso ERM, asegurando consistencia con el MIPG y el Sistema de Control Interno. Adopta y actualiza la metodología para la gestión de riesgos institucionales, incorporando de manera específica el componente de riesgo fiscal.

Es así como, el capítulo dedicado a este tipo de riesgo "fiscal" establece un paso a paso para su gestión (identificación, análisis y valoración), el cual se integra al esquema general de administración de riesgos de la entidad. Con ello, se busca disponer de un marco integral que facilite el seguimiento por parte de los líderes de proceso, y que asegure una administración más efectiva de los bienes, recursos e intereses distritales, previniendo impactos adversos y mitigando la posibilidad de responsabilidades fiscales.

Como insumo de referencia, la Alcaldía Distrital adopta el catálogo indicativo de puntos de riesgo fiscal y circunstancias inmediatas, construido a partir de:

- Fallos con responsabilidad fiscal en firme emitidos por Contralorías Territoriales y la Contraloría General de la República en los últimos tres años.
- Listados de hallazgos fiscales consolidados por la Auditoría General de la República.
- Análisis de tendencias y tipologías recurrentes en procesos de responsabilidad fiscal.

La metodología se articula con las siguientes fases:

- Fase 1. Política de Administración de Riesgos: La alta dirección definió los lineamientos en alineación con el esquema de líneas de defensa previsto en la dimensión 7 de control interno del MIPG. Este paso constituyó la base para la gestión integral del riesgo en todos los niveles de la entidad.
- Fase 2. Identificación de riesgos: Se plantea una redacción estructurada que facilita el análisis de causas raíz, evitando generalizaciones. Aquí se precisan factores de riesgo y su relación con tipologías distritales (gestión, fiscal, corrupción, seguridad de la información).

- Fase 3. Valoración de riesgos: Se establecen criterios para el análisis de probabilidad e impacto, considerando tanto la afectación económica como reputacional. La matriz de calor se ajusta con cinco niveles de severidad (bajo, moderado, alto y extremo), fortaleciendo la capacidad de análisis en un entorno cambiante.

El análisis de controles mantiene atributos de diseño y ejecución definidos en la versión 2 de la guía de riesgos, pero adiciona una tabla que permite calcular variaciones en la matriz de calor y medir la eficiencia de los controles aplicados, fortaleciendo el seguimiento por la Gerencia de Control Interno de Gestión y los órganos de control fiscal.

En los apartados finales se abordan las opciones de tratamiento del riesgo y los indicadores clave de riesgo (KRI) como herramienta de monitoreo y apoyo a la toma de decisiones.

De igual forma, en coherencia con las políticas nacionales, se mantienen y articulan los capítulos relacionados con:

- Transparencia, acceso a la información pública y lucha contra la corrupción (liderados a nivel nacional por la Secretaría de Transparencia).
- Seguridad de la información (alineada con el modelo del MINTIC).

Finalmente, los anexos incluyen:

- Catálogo indicativo de puntos de riesgo fiscal y circunstancias inmediatas.
- Matriz para la construcción del mapa de riesgos.
- Protocolo de identificación de riesgos de corrupción asociados a la prestación de trámites y servicios, en concordancia con la política de racionalización de trámites.
- Matriz de seguimiento a los riesgos de corrupción.

2. GENERALIDADES

2.1 OBJETIVO

Proveer lineamientos para identificar, analizar, valorar, tratar, monitorear y comunicar los riesgos de la entidad, protegiendo el logro de objetivos estratégicos, misionales y de apoyo.

2.2 ALCANCE

La guía tiene un alcance transversal a todos los procesos y niveles de la Alcaldía Distrital. Integra las tipologías de riesgo de gestión (operativos), fiscal, de corrupción y de seguridad de la información y es de aplicación tanto para servidores públicos como para contratistas. Su implementación se articula de manera directa con la planeación institucional, el presupuesto, la contratación y el seguimiento y evaluación al desempeño.

2.3 TÉRMINOS Y DEFINICIONES

TÉRMINOS RELATIVOS A LA GESTIÓN DE RIESGOS

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

Apetito del 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 del 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.

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

Control: Medida que mantiene o modifica el riesgo.

Nota: Los controles no siempre pueden producir el efecto de modificación previsto o asumido. Definición tomada de la ISO31000:2018.

Identificación del Riesgo: Proceso de análisis para encontrar una potencial desviación de los objetivos.

Factores de Riesgo: Son las fuentes generadoras de riesgos.

Gestión del Riesgo: Un proceso para identificar, evaluar, manejar y controlar acontecimientos o situaciones potenciales, con el fin de proporcionar un aseguramiento razonable respecto del alcance de los objetivos de la entidad.

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

Mapa de Riesgos: Documento que resume los resultados de las actividades de gestión de riesgos, incluye una representación gráfica en modo de mapa de calor de los resultados de la evaluación de riesgos.

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

Riesgo: Efecto de la incertidumbre sobre los objetivos.

Nota: Un efecto es una desviación respecto a lo previsto. Puede ser positivo, negativo o ambos, y puede abordar, crear o resultar en oportunidades y amenazas. Definición tomada de la ISO 31000:2018.

Riesgo Inherente: Aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

Riesgo Residual: El riesgo que permanece después de que la dirección haya realizado sus acciones para reducir el impacto y la probabilidad de un acontecimiento adverso.

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 del Riesgo: Proceso para modificar el riesgo.

Valoración del riesgo: Establece la identificación y evaluación de los controles. En la etapa de valoración del riesgo se determina el riesgo residual.

TÉRMINOS RELATIVOS A RIESGOS DE CORRUPCIÓN

Corrupción[1]**:** Abuso de posiciones de poder o de confianza, para el beneficio particular en detrimento del interés colectivo, realizado a través de ofrecer o solicitar, entregar o recibir bienes o dinero en especie, en servicios o beneficios, a cambio de acciones, decisiones u omisiones.

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.

TÉRMINOS RELATIVOS A RIESGOS FISCALES

Riesgo fiscal: Es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.[2] (Ver conceptos de recursos públicos, bien público e Intereses patrimoniales de naturaleza pública).

Bien público: Son todos aquellos muebles e inmuebles de propiedad pública (este concepto comprende: bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Estos se clasifican en bienes de uso público y bienes fiscales, definidos así:

a) Bien de uso público: aquellos cuyo uso pertenece a todos los habitantes del territorio nacional. Ejemplos: Las calles, plazas, puentes, vías, parques etc.

[1] Definición tomada de Transparencia por Colombia

[2] Concepto propuesto por Función Pública, a partir del análisis de fallos de responsabilidad fiscal.

b) Bienes fiscales: aquellos que están destinados al cumplimiento de las funciones públicas o servicios públicos (Consejo de Estado, 2012), es decir, afectos al desarrollo de su misión y utilizados para sus actividades.

Ejemplos: Los terrenos, edificios, oficinas, colegios, hospitales, otras construcciones, fincas, granjas, equipos, enseres, mobiliario etc.

Gestión del Riesgo Fiscal: Son las actividades que debe desarrollar cada entidad y todos los gestores públicos (ver concepto de gestor público) para identificar, valorar, prevenir y mitigar los riesgos fiscales (probabilidad de efecto dañoso sobre los bienes, recursos y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial).

Patrimonio público: Se entiende como el conjunto de bienes o recursos o intereses patrimoniales de naturaleza pública, susceptibles de estimación económica (artículo 6 Ley 610 de 2000 y sentencia C-340-07).

Punto de Riesgo: Actividades en las que potencialmente se genera riesgo. Tratándose de riesgo fiscal los puntos de riesgo son todas las actividades que representen gestión fiscal, por ejemplo, aquellas de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos o intereses de naturaleza pública.

Para la identificación y priorización de los puntos de riesgo, la entidad deberá tener en cuenta aquellas actividades en las cuales se han presentado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal, así como, aquellas actividades que la organización identifique que pueden generar riesgos fiscales. Para facilitar el ejercicio de identificación de puntos de riesgo consulte el Anexo: Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas.

Recurso público: Recurso público, los dineros comprometidos y ejecutados en ejercicio de la función pública.

Ejemplos: Los recursos de inversión y recursos de funcionamiento de cada entidad; los recursos generados por actividades comerciales, industriales y de prestación de servicios, por parte de entidades estatales; los recursos parafiscales; los recursos que resultan del ejercicio de funciones públicas por particulares.

TÉRMINOS RELATIVOS A RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

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, Tecnologías de la Información -TI- o Tecnologías de la Operación -TO-, entre otros, que utiliza la organización para su funcionamiento.

Amenazas: Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

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

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

TIC: Tecnologías de la Información y las Comunicaciones.

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

COMITÉS INSTITUCIONALES

CICCI: Comité Institucional de Coordinación de Control Interno.

CGDI: Comité de Gestión y Desempeño Institucional.

2.4 DOCUMENTOS DE REFERENCIA

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN – ICONTEC. Norma Técnica Colombiana NTC-ISO 31000 Gestión del riesgo — Directrices. 2018.

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PUBLICA - DAFP. Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de Gestión, Corrupción y Seguridad Digital. Versión 4. 2018.

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PUBLICA - DAFP. Guía para

la administración del riesgo y el diseño de controles en entidades públicas. Versión 6. 2022.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (MINTIC). Modelo Nacional de Gestión de Riesgos de Seguridad Digital (MGRSD).

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO) - Gestión del Riesgo Empresarial 2017.

3. PROCESO DE GESTIÓN DE RIESGOS

El proceso de la gestión del riesgo implica la aplicación sistemática de políticas, procedimientos y prácticas a las actividades de comunicación y consulta, establecimiento del contexto y evaluación, tratamiento, seguimiento, revisión, registro e informe del riesgo. Este proceso se ilustra en la siguiente gráfica.

Ilustración 1. Metodología para la administración del riesgo

Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 6. Pág. 22

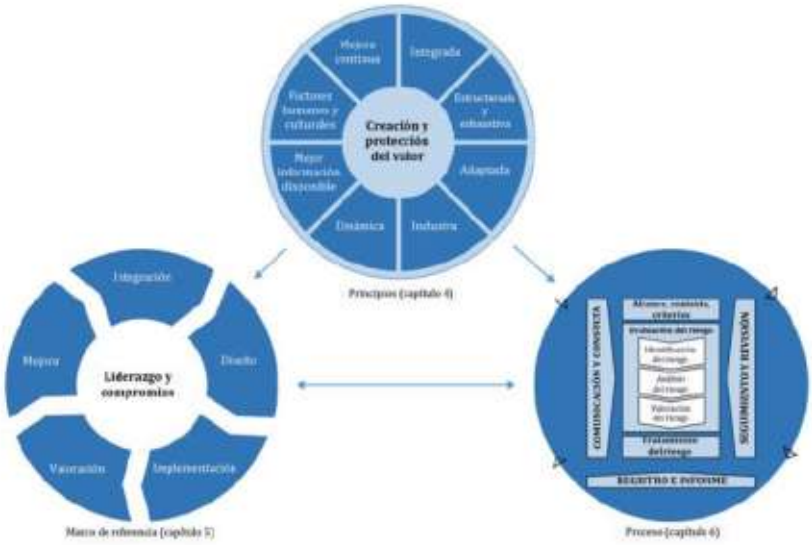
3.1 PRINCIPIOS PARA LA GESTIÓN DE RIESGOS

La Alcaldía Distrital de Barranquilla orientará la gestión del riesgo con base en los principios establecidos en la norma ISO 31000, enfocados en la creación y protección del valor público:

a. La gestión del riesgo crea y protege el valor: La gestión del riesgo contribuye al logro demostrable de los objetivos y a la mejora del desempeño en aspectos tales como seguridad humana, la conformidad legal y reglamentaria, la seguridad de la información, la aceptación pública, la protección del ambiente, la calidad de los servicios, la gestión de proyectos, la eficiencia en las operaciones, el buen gobierno, la probidad, la transparencia y la reputación.

b. La gestión del riesgo es sistemática, estructurada y oportuna: Un enfoque sistemático, oportuno y estructurado para la gestión del riesgo contribuye a la eficiencia y a resultados consistentes, comparables y confiables.
c. La gestión del riesgo es parte de la toma de decisiones: La gestión del riesgo ayuda a la alta dirección y los líderes de los procesos a hacer elecciones informadas, priorizar acciones y distinguir entre cursos de acción alternativos.
d. La gestión del riesgo es una parte integral de todos los procesos de la Entidad: La gestión del riesgo no es una actividad independiente que se separa de las actividades y los procesos principales de la organización.
e. La gestión del riesgo aborda explícitamente la incertidumbre: La gestión del riesgo toma en consideración explícitamente a la incertidumbre, su naturaleza y la forma en que se puede tratar.
f. La gestión del riesgo se basa en la mejor información disponible: Las entradas para el proceso de gestión del riesgo se basan en fuentes de información tales como datos históricos, experiencia, retroalimentación de las partes involucradas, observación, previsiones y examen de expertos. Sin embargo, quienes toman las decisiones deberían informarse y tomar en consideración todas las limitaciones de los datos o de los modelos utilizados, o la posibilidad de divergencia entre los expertos.
g. La gestión del riesgo está adaptada: La gestión del riesgo se alinea del contexto externo e interno y del perfil de riesgo de la Entidad.
h. La gestión del riesgo toma en consideración los factores humanos y culturales: La gestión del riesgo reconoce las capacidades, percepciones e intenciones de individuos externos e internos, los cuales pueden facilitar o dificultar el logro de los objetivos de la Entidad.
i. La gestión del riesgo es transparente e inclusiva: La correcta y oportuna intervención de las partes involucradas y, en particular, de aquellos que toman las decisiones en todos los niveles de la Entidad, garantiza que la gestión del riesgo siga siendo pertinente y se actualice. Esta intervención también permite a las partes interesadas estar correctamente representadas y hacer que sus puntos de vista se tomen en consideración al determinar los criterios del riesgo.
j. La gestión del riesgo es dinámica, reiterativa y receptiva al cambio: La gestión del riesgo siente y responde continuamente al cambio. A medida que se presentan los eventos externos e internos, el contexto y el conocimiento cambian, tienen lugar el monitoreo y la revisión de los riesgos, emergen riesgos nuevos, algunos cambian y otros desaparecen.

Ilustración 2. ISO31000 - Principios, marco de referencia y proceso



ISO (Organización Internacional de Normalización) - ISO 31000:2018. Gestión del riesgo. https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

3.2 IDENTIFICACIÓN DE RIESGOS

La identificación del riesgo constituye la primera fase del proceso de gestión de riesgos y busca reconocer de manera sistemática los eventos, condiciones o situaciones que puedan afectar, positiva o negativamente, el cumplimiento de los objetivos estratégicos o del proceso. Este ejercicio permite identificar tanto los riesgos que están bajo control de la organización como aquellos que escapan de su gestión directa, aportando insumos clave para su posterior análisis y valoración.

Para su desarrollo, se parte del contexto estratégico en el que opera la entidad, que incluye la misión, la visión, los objetivos del Plan de Desarrollo Distrital y las obligaciones normativas. De igual manera, se consideran los elementos de la caracterización de los procesos, tales como su objetivo, alcance, responsables, actividades, productos y recursos asociados, que sirven de base para identificar riesgos específicos en cada eslabón de la cadena de valor.

Adicionalmente, la etapa de Identificación exige un análisis integral de los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.

La técnica seleccionada para el análisis de factores internos y externos corresponde a la matriz DOFA – Contexto del Proceso.

📌*Nota: En caso de que el proceso cuente con una matriz DOFA previamente elaborada, será necesario que en cada vigencia esta se revise y actualice, incorporando, modificando o eliminando los aspectos internos o externos que deban ser considerados.*

3.2.1 ANÁLISIS DE OBJETIVOS ESTRATÉGICOS Y DE LOS PROCESOS

Este paso es muy importante, dado que todos los riesgos que se identifiquen deben tener impacto en el cumplimiento del objetivo estratégico o del proceso. La entidad debe analizar los objetivos estratégicos y revisar que se encuentren alineados con la misión y la visión institucionales, así como su desdoble hacia los objetivos de los procesos.

Ilustración 3. Análisis de objetivos

Análisis de objetivos estratégicos	Análisis de los objetivos de proceso
La entidad debe analizar los objetivos estratégicos e identificar los posibles riesgos que afectan su cumplimiento y que puedan ocasionar su éxito o fracaso. Es necesario revisar que los objetivos estratégicos se encuentren alineados con la Misión y la Visión Institucional, así como, analizar su adecuada formulación, es decir, que contengan las siguientes características mínimas: específico, medible, alcanzable, relevante y proyectado en el tiempo (SMART por sus siglas en inglés).	Los objetivos de proceso deben ser analizados con base en las características mínimas explicadas en el punto anterior, pero además, se debe revisar que los mismos estén alineados con la Misión y la Visión, es decir, asegurar que los objetivos de proceso contribuyan a los objetivos estratégicos. A continuación encontrará un ejemplo de análisis en el proceso de contratación: La entidad debe adquirir con oportunidad y calidad técnica, en no menos del 90%, los bienes y servicios requeridos para su continua operación.

Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 6. Pág. 22

📌*Nota: Los objetivos deben incluir el "qué", "cómo", "para qué", "cuándo", "cuánto". Si no están bien definidos los objetivos, no se puede continuar con la metodología de gestión del riesgo.*

3.2.2 IDENTIFICACIÓN DE LOS PUNTOS DE RIESGO

Corresponden a puntos críticos dentro del flujo del proceso en los que existe evidencia objetiva o indicios razonables de que pueden materializarse eventos de riesgo operativo. Estos eventos pueden estar asociados a fallas en el uso de insumos, en la ejecución de actividades, en la generación de productos o en la obtención de resultados e impactos.

Por ello, deben mantenerse bajo monitoreo y control permanente, a través de acciones preventivas, detectivas y correctivas, que aseguren que el proceso se desarrolla conforme a lo planeado.

La identificación de estos puntos críticos permite:

- Anticipar desviaciones que comprometan la eficiencia (relación entre insumos y productos).
- Prevenir afectaciones en la eficacia (cumplimiento de los objetivos).
- Garantizar la generación de valor[3] público, expresado en resultados y cambios positivos en la población objetivo.

Ilustración 4. Cadena de Valor

Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 6. Pág. 32

[3] Describe una relación secuencial y lógica entre insumos, actividades, productos y resultados, en la que se añade valor a lo largo del proceso de transformación total. Los insumos son los factores productivos, bienes o servicios con los que se cuenta para la generación de valor. Éstos pueden ser de tipo financiero, humano, jurídico, de capital, etc. Las actividades son el conjunto de procesos u operaciones mediante los cuales se genera valor al utilizar los insumos, dando lugar a un producto determinado. Los productos son los bienes y servicios provistos por el Estado que se obtienen de la transformación de los insumos a través de la ejecución de las actividades. Los resultados son los efectos relacionados con la intervención pública, una vez se han consumido los productos provistos por ésta. Los efectos pueden ser intencionales o no y/o atribuibles o no a la intervención pública. Los impactos son los efectos exclusivamente atribuibles a la intervención pública. (Tomado del documento "Guía Metodológica para el Seguimiento y la Evaluación a Políticas Públicas, elaborado por el DNP, 2014).

Nota: En consecuencia, estos puntos deben ser documentados en las matrices de riesgos institucionales, vinculados y desplegados en los controles existentes y a los responsables de su gestión, asegurando trazabilidad, control de las operaciones, transparencia y mejora continua en la cadena de valor público.

3.2.3 IDENTIFICACIÓN DE LAS ÁREAS DE IMPACTO

El área de impacto se entiende como la dimensión o esfera específica en la que se evidencian las consecuencias derivadas de la materialización de un riesgo. Estas consecuencias pueden comprometer de manera directa o indirecta el cumplimiento de los objetivos institucionales, la sostenibilidad de los recursos y la confianza de los grupos de valor.

La identificación de áreas de impacto permite valorar de forma más precisa los efectos de los riesgos, estableciendo una relación entre los eventos adversos y los activos, procesos o resultados que podrían ser afectados. De acuerdo con las directrices de la ISO 31000:2018 y el marco COSO ERM, este análisis es esencial para comprender no solo la probabilidad de ocurrencia, sino también la magnitud de sus consecuencias en términos cuantitativos y cualitativos.

En el marco de la Política de Administración de Riesgos de la Alcaldía Distrital de Barranquilla, se reconocen como impactos prioritarios los siguientes:

Impacto Económico: Hace referencia a la afectación sobre los recursos financieros de la entidad, ya sea por pérdida de ingresos, incremento de costos, sanciones, ineficiencia en la ejecución presupuestal, materialización de contingencias fiscales o disminución de la sostenibilidad financiera en el corto, mediano o largo plazo.

Impacto Reputacional: Corresponde a las consecuencias que un riesgo puede generar sobre la imagen, credibilidad y confianza de la ciudadanía y de los grupos de valor y/o interés en la gestión de la entidad. Una afectación reputacional puede impactar la legitimidad institucional, dificultar la articulación con aliados estratégicos y reducir la aceptación de políticas públicas.

3.2.4 IDENTIFICACIÓN DE ÁREAS DE FACTORES DE RIESGO

Los factores de riesgo son las fuentes generadoras de riesgos. Su identificación constituye un paso esencial, pues permite anticipar situaciones que pueden afectar el logro de los objetivos institucionales y orientar la definición de controles adecuados.

La identificación de factores debe realizarse teniendo en cuenta la naturaleza de la entidad, su nivel de complejidad, los procesos que desarrolla y el entorno en el que se encuentra. De acuerdo con la ISO 31000:2018 y el COSO ERM, los factores de riesgo corresponden a aquellos elementos internos y externos que, al interactuar con los procesos organizacionales, pueden generar desviaciones en el desempeño, pérdidas económicas, daños reputacionales o incumplimiento de los objetivos estratégicos.

La siguiente tabla, presentan ejemplos de factores de riesgo aplicables a entidades públicas:

Tabla 1. Factores de riesgo

Factor	Definición		Descripción
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.		- Falta de procedimientos Errores de grabación, autorización. - Errores en cálculos para pagos internos y externos. - Falta de capacitación, temas relacionados con el personal.
Talento humano	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.		- Hurto de activos. - Posibles comportamientos no éticos de los empleados. - Fraude interno (corrupción, soborno).
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.		- Daño de equipos. - Caída de aplicaciones. - Caída de redes. - Errores en programas.
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.		- Derrumbes. - Incendios. - Inundaciones. - Daños a activos fijos.
Evento externo	Situaciones externas que afectan a la entidad.		- Suplantación de identidad. - Asalto a la oficina. - Atentados, vandalismo, orden público.

Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 6. Pág. 33-34

📌*Nota: Los factores relacionados son una guía orientadora. La entidad debe analizar y ajustar aquellos que considere pertinentes, de acuerdo con su nivel de complejidad y con*

el sector en el que desarrolla su gestión. Este ejercicio resulta fundamental para incorporar los factores de riesgo más relevantes dentro del análisis de contexto.

3.2.5 DESCRIPCIÓN DEL RIESGO

La descripción del riesgo debe contener los elementos suficientes para que sea comprensible tanto para el líder del proceso como para personas externas al mismo. Con este propósito, se recomienda emplear una estructura estandarizada que facilite la redacción y brinde claridad. La propuesta inicia con la frase "POSIBILIDAD DE", seguida de los aspectos clave que caracterizan al riesgo.

Ilustración 5. Estructura de redacción para cualquier riesgo

Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 6. Pág. 34

Esta estructura contribuye a reducir la subjetividad en la redacción, permite visualizar la forma en que el riesgo puede materializarse y facilita la identificación de sus causas inmediatas y causas raíz. Dicha información es esencial para la definición de controles efectivos en la etapa de valoración del riesgo.

Desglosando la estructura propuesta tenemos:

- **Impacto:** corresponde a las consecuencias que la materialización del riesgo puede ocasionar a la organización, afectando sus objetivos, procesos, recursos o reputación.
- **Causa inmediata:** son las circunstancias o condiciones más visibles que explican cómo se presenta el riesgo, pero que no constituyen su origen principal.
- **Causa raíz:** es la causa fundamental o de base que origina el riesgo. Identificarla permite definir controles eficaces y sostenibles. Para un mismo riesgo pueden existir varias causas o sub-causas, las cuales deben ser analizadas de manera integral.

Ejemplo:

Proceso: gestión de recursos.

Objetivo: adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación.

Alcance: inicia con el análisis de necesidades para cada uno de los procesos de la entidad (plan anual de adquisidores) y termina con las compras y contratación requeridas bajo las especificaciones técnicas y normativas establecidas.

Atendiendo el esquema propuesto para la redacción del riesgo, tenemos:

Ilustración 6. Ejemplo aplicado bajo la estructura propuesta para la redacción del riesgo

Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 6. Pág. 36

Tabla 2. Premisas para una adecuada redacción del riesgo

Premisa	Incorrecto (Ejemplo de redacción inadecuada)
No describir como riesgos omisiones ni desviaciones del control	"Errores en la liquidación de la nómina por fallas en los procedimientos existentes."
No describir causas como riesgos	"Inadecuado funcionamiento de la plataforma estratégica donde se realiza el seguimiento a la planeación."
No describir riesgos como la negación de un control	"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	"Pérdida de expedientes" (como riesgo transversal).

Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 6. Pág. 36

Puede ser un riesgo asociado a la gestión documental, a la gestión contractual o jurídica y en cada proceso sus controles son diferentes.

3.2.6 CLASIFICACIÓN DEL RIESGO

La clasificación del riesgo permite agrupar los riesgos identificados y facilita su análisis, tratamiento y seguimiento. Cada riesgo se clasifica en una de las siguientes categorías:

Ilustración 7. Clasificación de riesgos

Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 6. Pág. 37

3.3 VALORACIÓN DEL RIESGO

La valoración del riesgo es una etapa central en el proceso de gestión de riesgos, ya que permite determinar el nivel de exposición de la entidad frente a los eventos identificados.

Este paso busca establecer, en primera instancia, la probabilidad de ocurrencia y las consecuencias o impactos del riesgo, con el fin de estimar el riesgo inherente.

Posteriormente, se evalúan los controles existentes para determinar el riesgo residual, es decir, el nivel de riesgo que permanece tras la aplicación de dichos controles.

La siguiente figura ilustra los componentes que conforman esta fase:

1. Análisis de riesgos: estimación del riesgo inicial (inherente) a partir de la probabilidad y el impacto.
2. Evaluación de riesgos: confrontación del riesgo analizado con los controles implementados, a fin de determinar el riesgo residual.

En la Alcaldía Distrital de Barranquilla, este ejercicio de valoración es esencial para priorizar riesgos, asignar recursos de manera eficiente y fortalecer la toma de decisiones estratégicas en concordancia con la Política de Administración de Riesgos y el Plan de Desarrollo Distrital.

Ilustración 8. Estructura para el desarrollo de la valoración del riesgo

Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 6. Pág. 39

3.3.1 ANÁLISIS DE RIESGOS

El Análisis de Riesgos tiene como propósito establecer la probabilidad de ocurrencia y las consecuencias o impactos que puede generar un evento de riesgo sobre los objetivos de la entidad. Este paso resulta esencial para priorizar riesgos y orientar la definición de medidas de control eficaces.

DETERMINAR LA PROBABILIDAD

La probabilidad se entiende como la posibilidad de ocurrencia del riesgo en un proceso o actividad específica. Para efectos de este análisis, la probabilidad estará asociada directamente con el nivel de exposición al riesgo que tiene el proceso o la actividad bajo revisión.

De esta manera, la probabilidad inherente se define como el número de veces que un proceso o actividad se enfrenta a un punto de riesgo durante un periodo de un (1) año.

Bajo este enfoque, se reduce la subjetividad que comúnmente afecta este tipo de análisis, ya que se fundamenta en la frecuencia real de exposición y no únicamente en la ocurrencia de eventos pasados.

Este esquema evita que, por ausencia de registros históricos, los riesgos se clasifiquen sistemáticamente en niveles bajos, situación que no refleja la verdadera realidad de la gestión pública en Colombia. En consecuencia, se obtiene un análisis más objetivo, transparente y ajustado al contexto institucional.

Como referente práctico, a continuación, se presenta una tabla de actividades típicas de la gestión pública, con sus respectivas escalas de probabilidad, que permitirá estandarizar el análisis y facilitar la comparación entre procesos.

Tabla 3. Actividades relacionadas con la gestión en entidades públicas

Actividad	Frecuencia de la Actividad	Probabilidad frente al Riesgo
Planeación estratégica	1 vez al año	Muy baja
Actividades de talento humano, jurídica, administrativa	Mensual	Media
Contabilidad, cartera	Semanal	Alta
Tecnología (incluye disponibilidad de aplicativos), tesorería 📌Nota: En materia de tecnología se tiene en cuenta 1 hora funcionamiento = 1 vez. Ej.: Aplicativo FURAG está disponible durante 2 meses las 24 horas, en consecuencia, su frecuencia se calcularía 60 días * 24 horas= 1440 horas.	Diaria	Muy alta

Construcción propia.

La Tabla 4 establece los criterios que permiten definir de manera objetiva el nivel de probabilidad, asegurando un análisis uniforme y consistente en el marco de la Política de Administración de Riesgos de la Alcaldía Distrital de Barranquilla.

Tabla 4. Criterios para definir el nivel de probabilidad

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

Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 6. Pág. 41

DETERMINAR EL IMPACTO

Para la tabla de criterios de impacto, se definen los impactos económicos y reputacionales como las variables principales de valoración. Es importante precisar que en la versión 2018 de la Guía de Administración del Riesgo del DAFP se contemplaban de manera diferenciada aspectos como: afectaciones a la ejecución presupuestal, pagos por sanciones económicas, indemnizaciones a terceros, sanciones por incumplimientos legales y afectaciones a la imagen institucional derivadas de vulneraciones de información o fallas en la prestación del servicio.

En la versión 2020 de la Guía, todos estos elementos se integran en dos dimensiones: impacto económico e impacto reputacional, simplificando y estandarizando el análisis. Un principio fundamental en este esquema es que, cuando un mismo riesgo presente impacto económico y reputacional con niveles distintos, debe tomarse siempre el nivel más alto. Por ejemplo: si para un riesgo se define un impacto económico en nivel insignificante y un impacto reputacional en nivel moderado, se tomará este último como referencia para la valoración.

De esta manera, se brinda a los líderes de proceso un instrumento objetivo y práctico para la estimación de los impactos, reduciendo la subjetividad que usualmente afecta este análisis.

Tabla 5. Criterios para definir el nivel de impacto

IMPACTO	DESCRIPCIÓN PRESUPUESTAL/IMPACTO ECONÓMICO	DESCRIPCIÓN REPUTACIONAL/IMPACTO CUALITATIVO	DESCRIPCIÓN LEGAL	DESCRIPCIÓN ESTRATÉGICO
Catastrófico 100%	Mayor a 500 SMLMV	Afectación de la imagen de la entidad y/o el Distrito de Barranquilla a nivel internacional	Genera sanciones para la entidad	Afecta el cumplimiento de la misión de la entidad
Mayor 80%	Entre 100 y 500 SMLMV	Afectación de la imagen de la entidad y/o el Distrito de Barranquilla a nivel nacional	Genera sanciones para uno o más funcionarios de la entidad	Afecta el cumplimiento de las metas distritales
Moderado 60%	Entre 50 y 100 SMLMV	Afectación de la imagen de la entidad y/o el Distrito de Barranquilla a nivel local	Genera investigaciones disciplinarias y/o fiscales y/o penales	Afecta el cumplimiento de los objetivos estratégicos de la entidad
Menor 40%	Entre 10 y 50 SMLMV	Afectación de uno o varios procesos de la entidad	Genera hallazgos administrativos	Afecta el cumplimiento de las iniciativas estratégicas
Leve 20%	Afectación menor a 10 SMLMV	Afectación de un grupo de servidores del proceso	Genera un requerimiento interno	Afecta el cumplimiento de algunas actividades contempladas en los planes de acción

Construcción propia.

Ejemplo (continuación):

Proceso: gestión de recursos

Objetivo: adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación

Riesgo identificado: posibilidad de afectación económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios fuera de los requerimientos normativos

N.° de veces que se ejecuta la actividad: la actividad de contratos se lleva a cabo 10 veces en el mes = 120 contratos en el año

Cálculo afectación económica: de llegar a materializarse, tendría una afectación económica de 500 SMLMV

Aplicando las tablas de probabilidad e impacto tenemos:

Probabilidad inherente: media 60%, **Impacto inherente:** mayor 80%

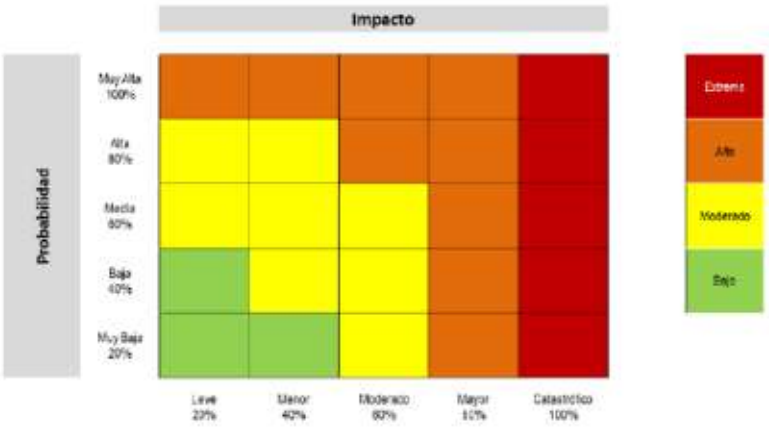
3.3.2 EVALUACIÓN DEL RIESGO

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial.

ANÁLISIS PRELIMINAR (RIESGO INHERENTE)

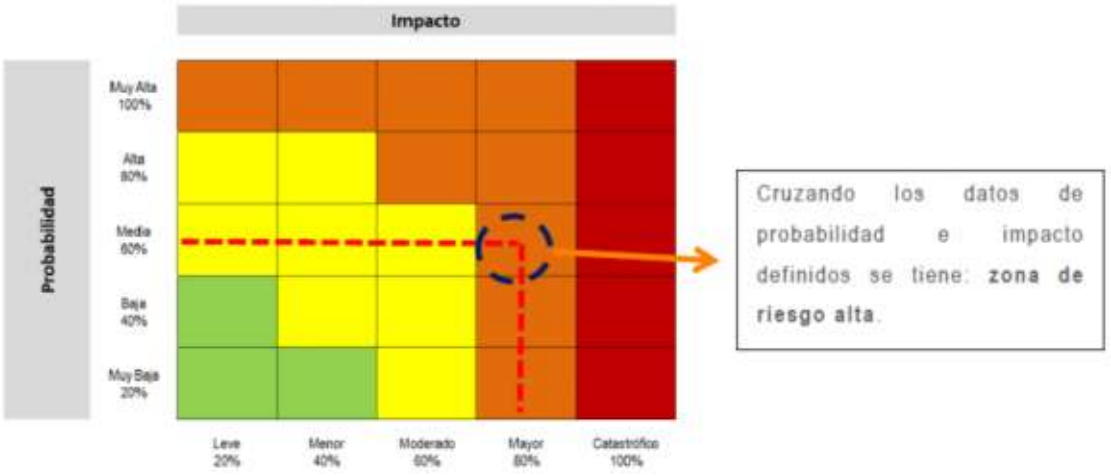
Se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor (probabilidad eje "Y" e impacto eje "X") que se muestra continuación:

Ilustración 9. Matriz de Calor (Niveles de Severidad del Riesgo)



Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 6. Pág. 44

Aplicando la matriz de calor al ejemplo tenemos:



VALORACIÓN DE CONTROLES

Los controles son medidas que permiten mantener o modificar el riesgo. Los controles actúan sobre alguna de las dos variables de su medición (probabilidad o impacto), bien sea para detectarlo a tiempo (evitar que se materialice) o reducirlo (minimizar las consecuencias). Las instrucciones y características para identificarlos junto con algunos ejemplos de controles de probabilidad e impacto se presentan a continuación. La valoración de los controles permite obtener una medida del éxito en su aplicación a través de su eficiencia (diseño) y su eficacia (logro del objetivo) en relación estrecha y directa de un riesgo en particular.

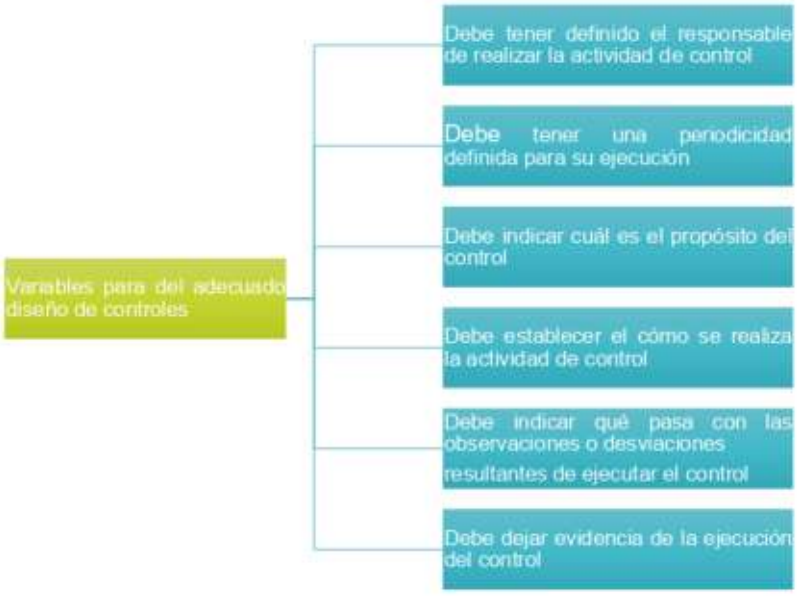
📌*Nota: A la hora de valorar los controles tenga en cuenta:*

- *Cuál es la variable que se espera mitigar con la aplicación del control (probabilidad o impacto).*
- *La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso sí aplica el criterio experto.*
- *Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.*
- *El exceso de controles implica sobrecostos para la entidad. Para qué controlar lo que ya se tiene controlado.*

Estructura para la descripción del control:

Para una adecuada redacción del control se propone una estructura que facilitará más adelante entender su tipología y otros atributos para su valoración. La estructura es la siguiente:

Ilustración 10. Diseño de controles



Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 4. Pág. 49

Se presenta a continuación un ejemplo de control bajo esta estructura:

Responsable	El profesional universitario 219 - 02
Periodicidad	cada vez que se va a realizar un contrato
Propósito	verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación
Cómo	a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor
Observaciones o Desviaciones	en caso de encontrar información faltante, requiere al proveedor a través de correo para el suministro de la información y poder continuar con el proceso de contratación
Evidencia	como evidencia deja Lista de Chequeo diligenciada con la información de la carpeta del cliente, y correos solicitando la información faltante en los casos que aplique

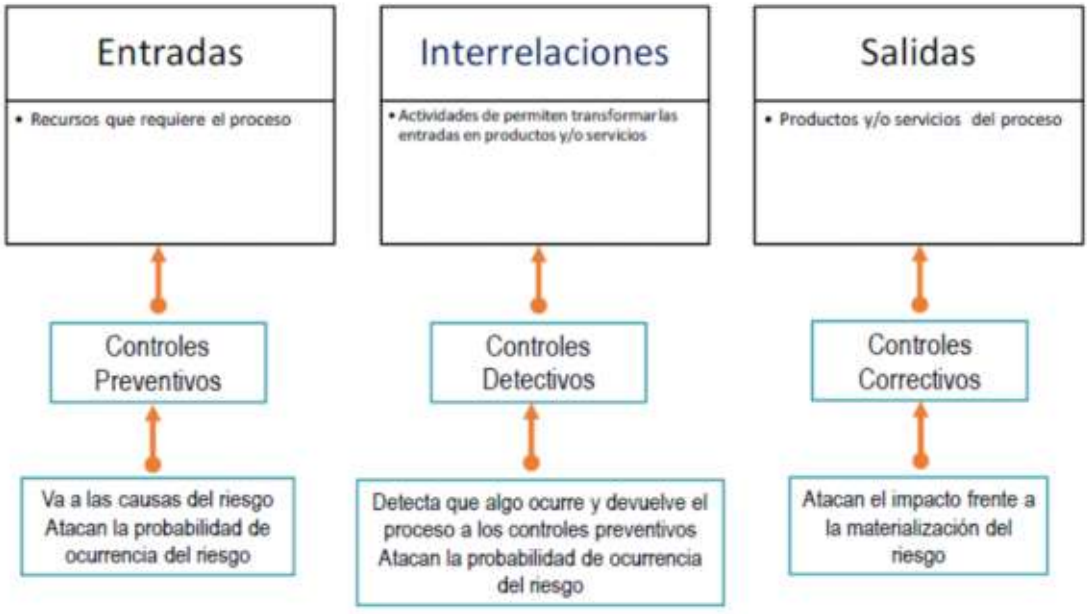
Nota: A la hora de diseñar los controles tenga en cuenta:

- *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, el sistema o aplicación (ej. Aplicativo de nómina, SIGEP).*
- *El control debe tener una periodicidad específica para su ejecución (diario, mensual, trimestral, anual).*
- *¿Para qué se realiza el control? (Verificar, validar, conciliar, comparar, revisar, cotejar, detectar, aprobar).*
- *¿Cómo se realiza el control? permite evaluar si la fuente u origen de la información que sirve para ejecutar el control es confiable para la mitigación del riesgo.*
- *La evidencia ayuda a que se pueda revisar la misma información por parte de un tercero y llegue a la misma conclusión de quien ejecutó el control.*

Tipología de controles y los procesos:

A través del ciclo de los procesos es posible establecer cuándo se activa un control y, por lo tanto, establecer su tipología con mayor precisión. Para comprender esta estructura conceptual, en la figura 11 se consideran 3 fases globales del ciclo de un proceso así:

Ilustración 11. Ciclo del proceso y las tipologías de controles



Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 6. Pág. 46

Acorde con lo anterior, tenemos las siguientes tipologías de controles:

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.

Control detectivo: control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.

Control correctivo: control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

Así mismo, de acuerdo con la forma como se ejecutan tenemos:

Control manual: controles que son ejecutados por personas.

Control automático: son ejecutados por un sistema.

Entendiendo las cualidades que posee un control, a continuación, se presentan algunos ejemplos de controles asociados a las variables de probabilidad e impacto:

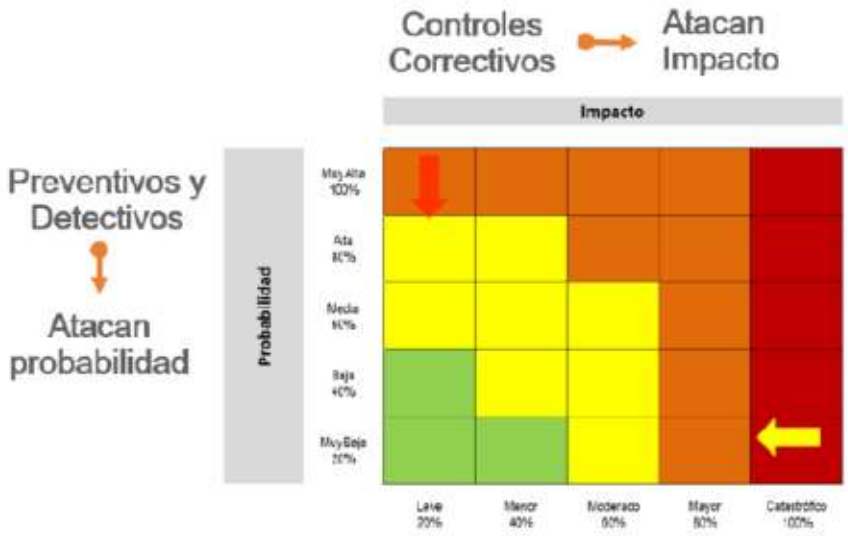
Tabla 6. Tipos de control para probabilidad e impacto

CONTROLES DE PROBABILIDAD: Recaen sobre la amenaza y tienen como objetivo principal evitar que el riesgo se materialice, por lo que se enfocan en atacar las causas detectadas en el análisis.	**CONTROLES DE IMPACTO:** Están enfocados en el activo amenazado, buscando reducir las consecuencias o efectos de la materialización del riesgo.
• Ejecución de programas de capacitación y entrenamiento. • Aplicación de listas de chequeo. • Verificación de firmas. • Aplicación de control dual. • Seguimiento o aplicación de normas, lineamientos y directrices. • Segregación de funciones. • Utilización de controles de acceso (lector de huellas, tarjetas inteligentes). • Revisiones y vistos buenos de superiores. • Elaboración, revisión o seguimiento a informes periódicos. • Ejecución o seguimiento a cronogramas, planes de trabajo. • Implantación de niveles de autorización en sistemas de información. • Registros de información. • Aplicación de procedimientos, manuales, guías e instructivos. • Realización de mantenimiento preventivo. • Activación de alertas de los sistemas de información. • Tercerización o subcontratación de actividades.	• Ejecución de auditorías internas o externas. • Puesta en marcha de planes de contingencia. • Ejecución de Backus o respaldos de información. • Análisis y medición de indicadores. • Realización de autoevaluaciones. • Confrontación de información para identificar diferencias (conciliaciones). • Ejecución de mantenimiento correctivo. • Retroalimentación a través de comités o reuniones periódicas. • Aplicación de pólizas y seguros. • Evaluación del desempeño. • Evaluación del grado de satisfacción de usuarios. • Inspecciones no programadas o seguimiento al reporte de PQRSD.

Construcción propia

Teniendo en cuenta que es a partir de los controles que se dará el movimiento, en la matriz de calor que corresponde a la ilustración 9 se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.

Ilustración 12. Movimiento en la matriz de calor acorde con el tipo de control



Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 6. Pág. 49

Análisis y evaluación de los controles – atributos:

A continuación, se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización. En la tabla 7 se puede observar la descripción y peso asociados a cada uno así:

Tabla 7. Atributos para el diseño del control

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

Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 6. Pág. 47-48

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

Ejemplo (continuación):

Proceso: gestión de recursos

Objetivo: adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación

Riesgo identificado: posibilidad de afectación económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos

Probabilidad Inherente= moderada 60%

Impacto Inherente: mayor 80%

Zona de riesgo: alta

Controles identificados:

Control 1: el profesional del área de contratos verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor, los contratos que cumplen son registrados en el sistema de información de contratación.

Control 2: el jefe del área de contratos verifica en el sistema de información de contratación la información registrada por el profesional asignado y aprueba el proceso para firma del ordenador del gasto, en el sistema de información queda el registro correspondiente, en caso de encontrar inconsistencias, devuelve el proceso al profesional de contratos asignado.

A continuación, se observa la aplicación de la tabla de atributos, esta le servirá como ejemplo para el análisis y valoración de los dos controles propuestos.

Control 1: El profesional del área de contratos verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor, los contratos que cumplen son registrados en el sistema de información de contratación.

Tabla de atributos	Peso
Tipo	
Preventivo	X – 25%
Detectivo	—
Correctivo	—
Implementación	
Automático	—
Manual	X – 15%
Documentación	
Documentado	X
Sin documentar	—
Frecuencia	
Continua	X
Aleatoria	—
Evidencia	
Con registro	X
Sin registro	—
Total, Valoración Control 1	40%

Control 2: El jefe del área de contratos verifica en el sistema de información de contratación la información registrada por el profesional asignado y aprueba el proceso para firma del ordenador del gasto, en el sistema de información queda el registro correspondiente, en caso de encontrar inconsistencias, devuelve el proceso al profesional de contratos asignado.

Tabla de atributos	Peso
Tipo	
Preventivo	—
Detectivo	X – 15%
Correctivo	—
Implementación	
Automático	—
Manual	X – 15%
Documentación	
Documentado	X
Sin documentar	—
Frecuencia	
Continua	X
Aleatoria	—
Evidencia	
Con registro	X

Sin registro	—
Total, Valoración Control 2	**30%**

NIVEL DE RIESGO (RIESGO RESIDUAL)

Es el resultado de aplicar la efectividad de los controles al riesgo inherente. Para la aplicación de los controles se debe tener en cuenta que los estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control.

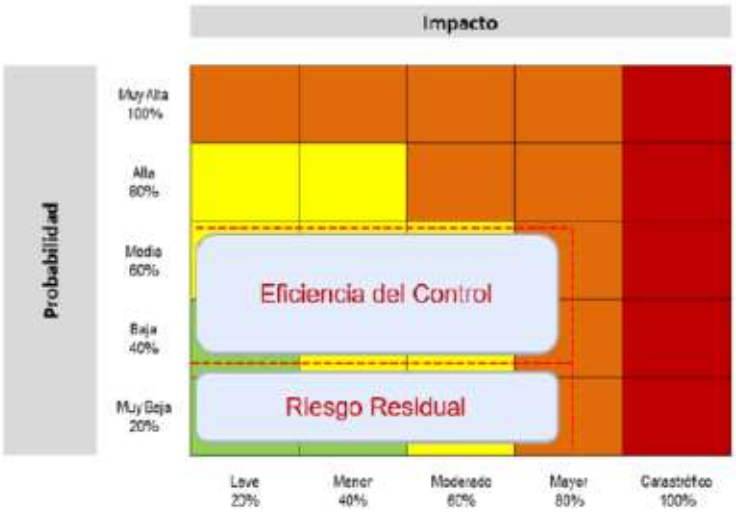
Para mayor claridad, en la ilustración 13 se da continuación al ejemplo propuesto, donde se observan los cálculos requeridos para la aplicación de los controles.

Ilustración 13. Aplicación de controles para establecer el riesgo residual

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
Posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos	Probabilidad inherente	60%	Valoración control 1 preventivo	40%	60%* 40% = 24% 60% - 24% = 36%
	Valor probabilidad para aplicar 2° control	36%	Valoración control 2 detectivo	30%	36%* 30% = 10,8% 36% - 10,8% = 25,2%
	Probabilidad Residual	25,2 %			
	Impacto Inherente	80%			
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	Impacto Residual	80%			

Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 6. Pág. 51

Para el caso del ejemplo, si bien el riesgo se mantiene en zona alta, se bajó el nivel de probabilidad de ocurrencia del riesgo. En la ilustración se observa el movimiento en la matriz de calor.



3.3.3 ESTRATEGIAS PARA COMBATIR EL RIESGO

El plan de tratamiento es la decisión que se toma e implementa frente a un determinado nivel de riesgo. La decisión puede ser ACEPTAR, REDUCIR, O EVITAR.

Ilustración 14. Estrategias para combatir el riesgo

Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 6. Pág. 58

El tratamiento del riesgo se aplicará cuando el riesgo residual se encuentre en nivel de severidad moderado, alto o extremo; para ello se definirá un plan de tratamiento con el objetivo de llevarlo a la zona de calificación baja. En este sentido, el plan de tratamiento

será un conjunto de acciones (actividades) que se ejecutarán en un periodo determinado de tiempo y buscará generar un nuevo control o modificar la eficiencia de un control existente. El formato dispuesto ante necesidades de tratamiento de riesgos es el EC-EC-F-068, Acciones Correctivas.

3.3.4 HERRAMIENTAS PARA LA GESTIÓN DE RIESGO

Como producto de la aplicación de la metodología institucional, se contará con los mapas de riesgo como instrumento principal. No obstante, para fortalecer el proceso de administración de riesgos de la Alcaldía Distrital de Barranquilla, se dispone también de las siguientes herramientas:

Gestión de eventos: Un evento corresponde a un riesgo materializado. Se consideran incidentes que han generado o podrían generar pérdidas para la entidad y que deben registrarse en una base histórica de eventos, la cual permite:

- Verificar si el riesgo fue previamente identificado.
- Analizar el desempeño de los controles implementados.
- Incluir en el mapa de riesgos aquellos que no hubiesen sido contemplados inicialmente, asignándoles el tratamiento correspondiente.

Ilustración 15. Fuentes base histórica de eventos

Construcción propia

Este mecanismo es fundamental para aprender de la experiencia institucional, evitar la recurrencia de incidentes y medir el desempeño de los controles, el cual puede calcularse con la siguiente fórmula:

Desempeño del control = N.º de eventos / Frecuencia del riesgo (N.º de veces que se realiza la actividad).

Nota: Para la identificación y reporte de eventos tener en la cuenta los lineamientos establecidos en el capítulo 8 de la política de administración de riesgos versión 4: Acciones ante los riesgos materializados.

Indicadores Clave de Riesgo (KRI): Los indicadores clave de riesgo (KRI), por sus siglas en inglés) corresponden a una colección de datos históricos, registrados por periodos de tiempo, que permiten anticipar una mayor o menor exposición a riesgos específicos.

- No representan la materialización del riesgo, pero sí sugieren desviaciones o fallas que deben investigarse.
- Facilitan la identificación temprana de tendencias negativas y constituyen señales de alerta para la toma de decisiones.
- Permiten capturar la ocurrencia de incidentes vinculados con riesgos previamente identificados y clasificados como altos, generando un registro que, al ser analizado en su evolución, evidencia la eficacia de los controles adoptados por la entidad.

A continuación, se presentan ejemplos de indicadores clave de riesgo que sirven como guía para su aplicación en los procesos de la Alcaldía Distrital de Barranquilla.

Tabla 8. Ejemplos indicadores clave de riesgo

Proceso Asociado	Indicador	Métrica
Gestión de las tecnologías de la información	Tiempo de interrupción de aplicativos críticos en el mes	Número de horas de interrupción de aplicativos críticos al mes
Gestión de recursos financieros	Reportes emitidos al regulador fuera del tiempo establecido	Número de reportes mensuales remitidos fuera de términos
Atención al Ciudadano	Reclamos de usuarios por incumplimiento a términos de ley o reiteraciones de solicitudes por conceptos no adecuados	% de solicitudes mensuales fuera de términos % de solicitudes reiteradas por tema

Proceso Asociado	Indicador	Métrica
Gestión de recursos financieros	Errores en transacciones y su impacto en la gestión presupuestal	Volumen de transacciones al mes sobre la capacidad disponible
Gestión de la Contratación	Incumplimiento de contratos	% de contratos con adiciones de tiempo o valor Número de sanciones contractuales aplicadas
Direccionamiento estratégico y planeación	Retrasos en ejecución de obras o proyectos	% de proyectos fuera de cronograma % de recursos no ejecutados frente al presupuesto asignado
Gestión de recursos financieros	Hallazgos con incidencia fiscal	Número de hallazgos con presunta incidencia fiscal identificados por la Contraloría Valor de los hallazgos sobre el presupuesto ejecutado
Gestión de las tecnologías de la información	Incidentes de ciberseguridad	Número de intentos de acceso no autorizado Tiempo promedio de recuperación tras incidentes de seguridad

Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 6. Pág. 60

3.3.5 MONITOREO Y REVISIÓN

Debido a que los riesgos no son estáticos y pueden cambiar de forma radical sin previo aviso, se requiere seguimiento y revisión durante todas las etapas del proceso por parte de los líderes de los procesos y la segunda línea de defensa de la entidad para:

- Garantizar la eficacia de los controles implementados.
- Obtener información adicional que permita mejorar la evaluación del riesgo.
- Detectar cambios en el contexto interno y externo.
- Identificar riesgos emergentes.
- Gestionar los riesgos materializados.
- Determinar el grado de cumplimiento en la ejecución de los planes de tratamiento propuestos.

Para el caso particular de los riesgos de gestión (operativos) se le hará seguimiento por parte de los líderes de los procesos atendiendo lo dispuesto en la Política de Administración de Riesgos de la entidad:

Tabla 9. Periodicidad de seguimiento a los riesgos de gestión

ZONA DE RIESGO RESIDUAL	ESTRATEGIA DE SEGUIMIENTO
Baja	Se realiza seguimiento trimestral y se registran sus avances en el módulo de riesgos en la herramienta tecnológica dispuesta para tal fin.
Moderada	Se realiza seguimiento trimestral y se registran sus avances en el módulo de riesgos en la herramienta tecnológica dispuesta para tal fin.
Alta	Se realiza seguimiento bimensual y se registran sus avances en el módulo de riesgos de la herramienta tecnológica dispuesta para tal fin.
Extrema	Se realiza seguimiento mensual y se registra en el módulo de riesgos de la herramienta tecnológica dispuesta para tal fin.

Política Administración de Riesgos Alcaldía Distrital de Barranquilla versión 4. Pág. 34

Una vez al año los líderes de los procesos, en conjunto con su equipo de colaboradores en los demás niveles jerárquicos, los agentes de cambio y equipos de mejoramiento continuo realizarán una revisión integral del proceso de gestión de sus riesgos (contexto, mapa de riesgos y planes de tratamiento). El periodo establecido para la revisión está comprendido entre los meses de febrero y marzo (a más tardar 31 de marzo de cada vigencia).

A continuación, se presentan los informes que se realizarán cada año para hacer seguimiento a la gestión institucional de los riesgos operativos:

Informe/reporte	Responsable	Dirigida a	Periodo de envió
Informe General Gestión del Riegos Institucional	Secretaria Distrital de Planeación	Miembros de Comité Institucional de Gestión y Desempeño	A más tardar el 28 febrero (El informe corresponde al año anterior)
Revisión y Evaluación – Riesgos de Gestión	Gerencia de Control Interno de Gestión	Líderes de proceso Miembros de Comité Institucional de Gestión y Desempeño Miembros de Comité Institucional de Coordinación de Control Interno	Diciembre

La divulgación y socialización de la Política y metodología de administración del riesgo y el mapa de riesgos institucional, estará a cargo de la Secretaría Distrital de Planeación con el apoyo de la Secretaría Distrital de Comunicaciones. La divulgación de los mapas de riesgos estará a cargo de los responsables de cada proceso, con el apoyo de los agentes de cambio y los equipos de mejoramiento continuo.

Evaluación Independiente de la efectividad de controles: La Gerencia de Control Interno de Gestión realizará, en el marco de sus roles y competencias, evaluación a la efectividad de los controles asociados al mapa de riesgos de los procesos, a través del formato "evaluación de efectividad de controles".

La efectividad de los controles se calculará con la siguiente fórmula:

$$\text{Efectividad} = \frac{\text{Eficiencia} + \text{Eficacia}}{2}$$

Eficiencia: Permite determinar que tan bien diseñado está un control. Los factores para estimar la eficiencia se deben calificar para cada control arrojando un valor numérico de 0 y 100, como se muestra a continuación.

Tabla 10. Análisis y evaluación de los controles

Criterio de Evaluación	Opción de Respuesta al Criterio de Evaluación	Peso en la Evaluación del Diseño del control
Asignación del responsable	Asignado	15
	No Asignado	0
Segregación y autoridad del responsable	Adecuado	0
	Inadecuado	15
Periodicidad	Oportuna	15
	Inoportuna	0
Propósito	Prevenir	15
	Detectar	10
	Corregir	5
	No es 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 Ejecución del Control	Completa	10
	Incompleta	5
	No Existe	0

Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 4. Pág. 61

La sumatoria del peso de la evaluación del diseño del control permite estimar la calificación, de acuerdo con la siguiente tabla:

Tabla 11. Resultado de la evaluación del diseño del control

Rango de calificación del diseño	Opción de respuesta al Criterio de Evaluación
Fuerte	Calificación entre 96 y 100
Moderado	Calificación entre 86 y 95
Débil	Calificación entre 0 y 85

Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 4. Pág. 62

Eficacia: Permite determinar el correcto funcionamiento del control. Los factores para estimar la eficacia se deben calificar para cada control arrojando un valor numérico de 0 y 100, como se muestra a continuación.

Tabla 12. Resultados de la evaluación de la ejecución del control

Rango de Calificación de la Ejecución	Opción de Respuesta al Criterio de Evaluación	Peso en la evaluación de la eficacia del control
Fuerte	El control se ejecuta de manera consistente por parte del responsable	100
Moderado	El control se ejecuta algunas veces por parte del responsable	50
Débil	El control no se ejecuta de manera consistente por parte del responsable	0

Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 4. Pág. 62

El promedio de la calificación de la eficiencia y eficacia del control se ubicará en la siguiente escala de colores para determinar su efectividad:

Tabla 13. Calificación efectividad del control

Calificación de Efectividad del Control	Rango de Efectividad	Color	Descripción
Alta	>=75		El control presenta un diseño y funcionamiento optimo
Media	Entre el 74 y 50		El control presenta un buen diseño y funcionamiento, susceptible de ser mejorado
Baja	<=49		El control presenta deficiencias en su diseño y funcionamiento, definir acciones de mejoramiento.

Construcción propia


RIESGOS
RELACIONADOS CON POSIBLES
ACTOS DE CORRUPCIÓN

4. LINEAMIENTOS SOBRE LOS RIESGOS RELACIONADOS CON POSIBLES ACTOS DE CORRUPCIÓN

En materia de riesgos asociados a posibles actos de corrupción, para la presente guía se consideran los siguientes aspectos:

- El 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. Esto implica que las prácticas corruptas son realizadas por actores públicos y/o privados con poder e incidencia en la toma de decisiones y la administración de los bienes públicos (CONPES N° 167 de 2013).
- Los riesgos de corrupción se establecen sobre procesos.
- El riesgo debe estar descrito de manera clara y precisa. Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos.

📌*Nota: Para la gestión de riesgos de corrupción, continúan vigentes los lineamientos contenidos en la versión 4 de la Guía para la Administración del Riesgo y el Diseño de controles en Entidades Públicas de 2018.*

4.1 GENERALIDADES SOBRE LA GESTIÓN DE RIESGOS DE CORRUPCIÓN

La gestión del riesgo de corrupción constituye un pilar estratégico de la transparencia y la integridad en la administración pública, en línea con los compromisos nacionales e internacionales suscritos por Colombia. Este ejercicio no solo responde a la obligación normativa, sino también al imperativo ético de proteger el patrimonio público y consolidar la confianza ciudadana en la gestión gubernamental.

- **Entidades responsables de la gestión del riesgo de corrupción:** La gestión de este riesgo corresponde a todas las entidades del orden nacional, departamental, distrital y municipal. En el caso de la Alcaldía Distrital de Barranquilla, cada proceso debe asegurar la identificación, análisis y tratamiento de los riesgos de corrupción en el marco de sus competencias, bajo la orientación de la Secretaría Distrital de Planeación y con el acompañamiento y asesoría de la Gerencia de Control Interno de Gestión.
- **Elaboración y consolidación del mapa de riesgos de corrupción:** Cada responsable de proceso, junto con su equipo, debe elaborar anualmente el mapa de riesgos de corrupción. La Secretaría Distrital de Planeación será la instancia encargada de liderar la consolidación y asegurar la coherencia metodológica del proceso, mientras que la Gerencia de Control Interno de Gestión verificará y evaluará que los lineamientos de control interno y autocontrol se apliquen de forma adecuada.

- **Publicación y acceso a la información:** El mapa de riesgos de corrupción debe ser publicado en la página web institucional, en la sección de Transparencia y Acceso a la Información Pública, en cumplimiento del artículo 2.1.1.2.1.4 del Decreto 1081 de 2015, a más tardar el 31 de enero de cada vigencia. La publicación será parcial y deberá respetar los criterios de clasificación y reserva previstos en los artículos 18 y 19 de la Ley 1712 de 2014, lo cual implica anonimizar la información clasificada.
- **Socialización:** Previo a la publicación, los servidores públicos y contratistas deben conocer el mapa de riesgos de corrupción. La Secretaría Distrital de Planeación deberá diseñar e implementar mecanismos de difusión interna (capacitaciones, talleres, mesas de trabajo), garantizando la participación de los equipos técnicos. De manera complementaria, la Gerencia de Control Interno de Gestión velará por la transparencia del proceso, promoviendo espacios de socialización externa con ciudadanía y grupos de valor, dejando evidencia del ejercicio y publicando los resultados.
- **Ajustes y modificaciones:** Durante la vigencia, el mapa podrá ser objeto de ajustes derivados de cambios en el contexto, hallazgos de auditoría, recomendaciones de entes de control o aportes ciudadanos. Dichas modificaciones deberán documentarse y contar con la validación de la Secretaría Distrital de Planeación y la Gerencia de Control Interno de Gestión.
- **Monitoreo:** Los líderes de proceso deben realizar monitoreo permanente de los riesgos de corrupción y reportar a la Secretaría Distrital de Planeación, quien consolidará los avances. La Gerencia de Control Interno de Gestión, en coherencia con su rol de tercera línea de defensa, evaluará la efectividad de los controles y la pertinencia de las acciones de mitigación.
- **Seguimiento y auditoría interna:** La Gerencia de Control Interno de Gestión incluirá dentro de sus planes de auditoría la verificación de la gestión de riesgos de corrupción, analizando causas, controles y efectividad de las medidas adoptadas. Este seguimiento constituye un insumo clave para la rendición de cuentas y el fortalecimiento de la cultura de integridad en el Distrito.

4.2. IDENTIFICACIÓN DE RIESGOS

A manera de ilustración a continuación se señalan algunos de los procesos, procedimientos o actividades susceptibles de actos de corrupción, a partir de los cuales la entidad podrá adelantar el análisis de contexto interno para la correspondiente identificación de los riesgos:

Tabla 14. Procesos, procedimientos o actividades susceptibles de riesgos de corrupción

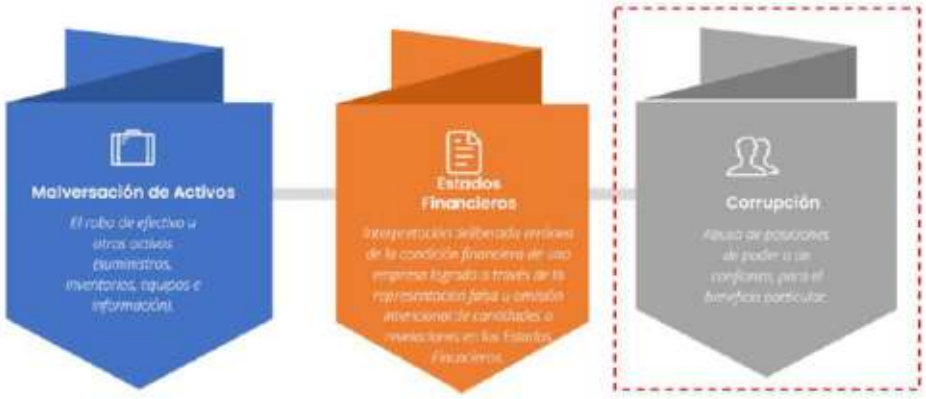
Secretaría de Transparencia de la Presidencia de la República, 2018

Direccionamiento estratégico (alta dirección)	▪ Concentración de autoridad o exceso de poder. Extralimitación de funciones. ▪ Ausencia de canales de comunicación. ▪ Amiguismo y clientelismo.
Financiero (está relacionado con áreas de planeación y presupuesto)	▪ Inclusión de gastos no autorizados. ▪ Inversiones de dineros públicos en entidades de dudosa solidez financiera a cambio de beneficios indebidos para servidores públicos encargados de su administración. ▪ Inexistencia de registros auxiliares que permitan identificar y controlar los rubros de inversión. ▪ Inexistencia de archivos contables. ▪ Afectar rubros que no corresponden con el objeto del gasto en beneficio propio o a cambio de una retribución económica.
De contratación (como proceso o bien los procedimientos ligados a este)	▪ Estudios previos o de factibilidad deficientes. ▪ Estudios previos o de factibilidad manipulados por personal interesado en el futuro proceso de contratación. *(Estableciendo necesidades inexistentes o aspectos que benefician a una firma en particular).* ▪ Pliegos de condiciones hechos a la medida de una firma en particular. ▪ Disposiciones establecidas en los pliegos de condiciones que permiten a los participantes direccionar los procesos hacia un grupo en particular. ▪ Visitas obligatorias establecidas en el pliego de condiciones que restringen la participación. ▪ Adendas que cambian condiciones generales del proceso para favorecer a grupos determinados. ▪ Urgencia manifiesta inexistente. ▪ Concentrar las labores de supervisión en poco personal. ▪ Contratar con compañías de papel que no cuentan con experiencia.
De información y documentación	▪ Ausencia o debilidad de medidas y/o políticas de conflictos de interés. ▪ Concentración de información de determinadas actividades o procesos en una persona. ▪ Ausencia de sistemas de información que pueden facilitar el acceso a información y su posible manipulación o adulteración. ▪ Ocultar la información considerada pública para los usuarios. ▪ Ausencia o debilidad de canales de comunicación.
De Investigación y sanción	▪ Inexistencia de canales de denuncia interna o externa. ▪ Dilatar el proceso para lograr el vencimiento de términos o la prescripción de este. ▪ Desconocimiento de la ley mediante interpretaciones subjetivas de las normas vigentes para evitar o postergar su aplicación. ▪ Exceder las facultades legales en los fallos.
De trámites y/o servicios internos y externos	▪ Cobros asociados al trámite. ▪ Influencia de tramitadores. ▪ Tráfico de influencias: (amiguismo, persona influyente).
De reconocimiento de un derecho (expedición de licencias y/o permisos)	▪ Falta de procedimientos claros para el trámite. ▪ Imposibilitar el otorgamiento de una licencia o permiso. ▪ Tráfico de influencias: (amiguismo, persona influyente).

📌*Nota: De acuerdo con el Marco Internacional para la Práctica Profesional de la Auditoría Interna (MIPP), los riesgos de corrupción hacen parte de una de las tres tipologías de riesgos de fraude, los cuales se entienden como:*

"Cualquier acto ilegal caracterizado por el engaño, la ocultación o la violación de la confianza. No requieren la utilización de la fuerza o de amenazas de violencia. El fraude puede ser cometido tanto por individuos como por organizaciones con el propósito de obtener dinero, bienes o servicios, evitar pagos u obligaciones, o bien asegurar ventajas personales o empresariales. El riesgo de fraude corresponde a la probabilidad de que este ocurra y a las consecuencias o impactos que pueda generar en la organización".

Ilustración 16. Árbol del Fraude



Marco Internacional para la Práctica profesional de Auditoría Interna

Con el propósito de facilitar la identificación de riesgos de corrupción y evitar confusiones frente a los riesgos de gestión, se recomienda la utilización del siguiente esquema de definición de riesgo de corrupción, dado que integra de manera explícita cada uno de los componentes que lo conforman.

Ilustración 17. Estructura para la redacción de riesgos de corrupción

Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 6. Pág. 84

A continuación, se presenta un ejemplo de riesgo de corrupción:

Ilustración 18. Ejemplo de redacción de riesgo de corrupción

Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 6. Pág. 84

4.3 VALORACIÓN DE RIESGOS

4.3.1 ANÁLISIS DE LA PROBABILIDAD

La probabilidad del riesgo se analiza en función de qué tan posible es que este ocurra, y puede expresarse en dos dimensiones: frecuencia o factibilidad.

- Frecuencia: corresponde al análisis del número de veces que un riesgo se ha materializado en un periodo determinado. Implica considerar el historial de situaciones o eventos asociados, lo cual permite identificar patrones de ocurrencia y establecer tendencias de comportamiento.
- Factibilidad: hace referencia a la posibilidad de ocurrencia de un riesgo aun cuando este no se haya presentado en el pasado. En este caso, el análisis se enfoca en los factores internos y externos que pueden propiciarlo, evaluando el entorno organizacional, normativo, tecnológico o social que incrementa la probabilidad de su materialización.

Tabla 15. Criterios para calificar la probabilidad

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
5	**Casi seguro**	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
4	**Probable**	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
3	**Posible**	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
2	**Improbable**	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
1	**Rara vez**	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 6. Pág. 84

4.3.2 ANÁLISIS DEL IMPACTO

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

Tabla 16. Criterios para calificar el impacto en riesgos de corrupción

	PREGUNTA:	RESPUESTA	
N°	**SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...**	**Si**	**No**
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de misión de la entidad?		
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad		
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		
9	¿Generar pérdida de información de la entidad?		
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?		
11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		
14	¿Dar lugar a procesos penales?		
15	¿Generar pérdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		
Responder afirmativamente de UNA a CINCO preguntas genera un impacto MODERADO Responder afirmativamente de SEIS a ONCE preguntas genera un impacto MAYOR Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto CATASTRÓFICO			
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad		
CATASTRÓFICO	Genera consecuencias desastrosas para la entidad		

Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 6. Pág. 88

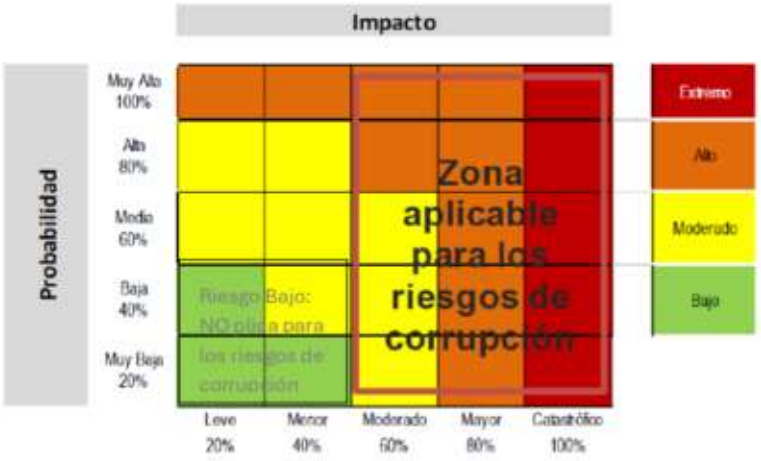
📌 *Nota: Si la respuesta a la pregunta 16 es afirmativa, el riesgo se considera CATASTRÓFICO.*

📌 *Nota: Por cada riesgo de corrupción identificado se debe diligenciar la tabla "Criterios para calificar el impacto en riesgos de corrupción".*

📌 *Nota: Para la determinación del impacto frente a posibles materializaciones de riesgos de corrupción se analizarán únicamente los siguientes niveles i) moderado, ii) mayor, y iii) catastrófico, dado que estos riesgos siempre serán significativos. En tal sentido, no aplican los niveles de impacto insignificante y menor, que sí aplican para las demás tipologías de riesgos.*

Una vez determinada la probabilidad y el impacto correspondiente, se deberá ubicar el riesgo en el mapa de calor institucional, identificando el punto de intersección entre ambas variables. Este ejercicio permitirá establecer el nivel de riesgo inherente, insumo fundamental para definir los planes de tratamiento, las medidas de mitigación y los controles a implementar en la Alcaldía Distrital de Barranquilla, en coherencia con los preceptos de integridad y transparencia.

Ilustración 19. Matriz de calor para riesgos de corrupción



Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 6. Pág. 89

4.4 VALORACIÓN DE LOS CONTROLES – DISEÑO DE CONTROLES

Para el diseño y valoración de controlesCriterios para definir el nivel de impactoCriterios para definir el nivel de impactoCriterios para definir el nivel de impactoCriterios para definir el nivel de impactoCriterios para definir el nivel de impactoCriterios para definir el nivel de impacto, se deberán observar los parámetros definidos

en la Versión 4 de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas (DAFP, 2018)[4], los cuales mantienen plena vigencia y aplicación en la gestión pública. Estos parámetros están definidos en el numeral 3.3.2 de esta guía.

En consecuencia, se recomienda a las dependencias responsables remitirse expresamente a dicho documento como referencia obligatoria, a fin de garantizar:

- La coherencia metodológica,
- La uniformidad en la aplicación de criterios y
- La alineación con las disposiciones nacionales en materia de control interno y gestión de riesgos.

Nivel del riesgo (riesgo residual)

Desplazamiento del riesgo inherente para calcular el riesgo residual

Nota: Tratándose de riesgos de corrupción únicamente hay disminución de probabilidad. Es decir, para el impacto no opera el desplazamiento.

4.5 TRATAMIENTO DEL RIESGO

El tratamiento del riesgo constituye la respuesta definida por la primera línea de defensa para la mitigación de los diferentes riesgos a los que se expone la entidad, incluyendo aquellos asociados a la corrupción.

En el momento de evaluar las opciones de tratamiento, y en coherencia con lo establecido en la política institucional de administración del riesgo, los responsables de proceso deberán considerar:

- La importancia del riesgo en función de su probabilidad e impacto.
- El efecto potencial sobre el logro de los objetivos institucionales.
- La relación costo–beneficio de las medidas a implementar.

De manera particular, frente a los riesgos de corrupción, la entidad priorizará respuestas orientadas a evitar, compartir o reducir el riesgo, en concordancia con los estándares

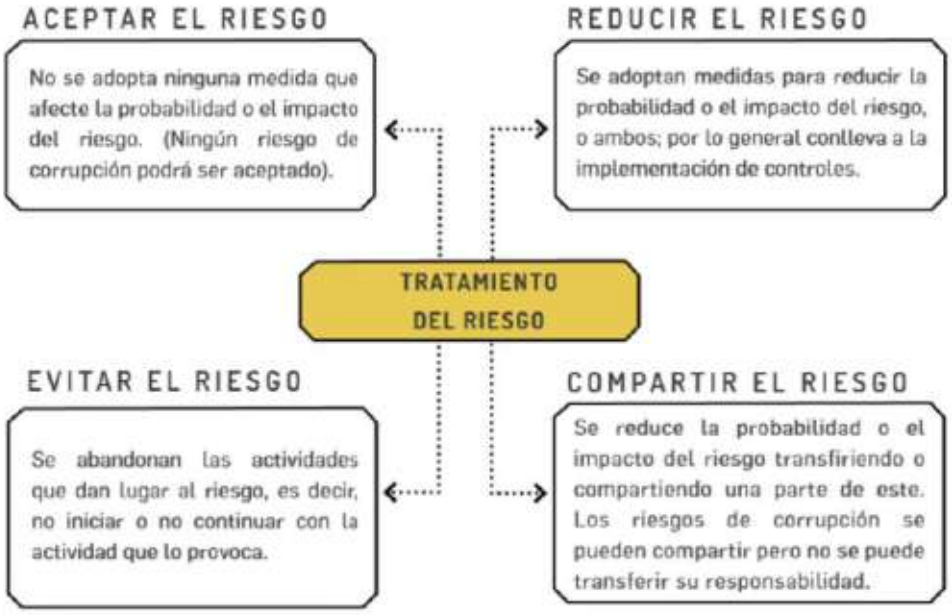
[4] Departamento Administrativo de la Función Pública – DAFP. *Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas*, Versión 4, octubre de 2018

nacionales de transparencia y las disposiciones del Modelo Integrado de Planeación y Gestión – MIPG.

El tratamiento o respuesta adoptada se enmarca en las siguientes categorías:

1. Evitar el riesgo: eliminar la causa o situación que lo origina.
2. Reducir el riesgo: implementar controles que disminuyan la probabilidad o impacto.
3. Compartir el riesgo: transferir parte del riesgo a terceros (seguros, alianzas, contratos).
4. Aceptar el riesgo: asumirlo, siempre que se encuentre dentro de los niveles de apetito y tolerancia institucionalmente definidos.

Ilustración 20. Tratamiento del riesgo



Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 6. Pág. 91

Nota: Es importante tener en cuenta que para los riesgos de corrupción no hay aceptación del riesgo.

Evitar el riesgo

Cuando los escenarios de riesgo identificados se consideran demasiado extremos, la entidad podrá optar por el tratamiento de evitar el riesgo, lo cual implica la cancelación de una actividad o de un conjunto de actividades que originan la amenaza.

Desde la perspectiva de los responsables de la toma de decisiones, esta alternativa constituye la más simple, menos arriesgada y costosa en términos de mitigación. Sin embargo, también puede representar un obstáculo para el cumplimiento de las metas institucionales, por lo cual su aplicación debe analizarse con especial rigor.

En consecuencia, el evitar el riesgo solo será una opción válida cuando:

- La magnitud del riesgo supera los niveles de apetito y tolerancia definidos por la Alta Dirección.
- No existan medidas de reducción o transferencia que resulten viables en términos de costo–beneficio.
- La suspensión de la actividad no comprometa el logro de objetivos estratégicos de la entidad ni el interés general.

De este modo, la decisión de evitar el riesgo debe adoptarse de manera excepcional, justificada y documentada, garantizando que no se convierta en una práctica que limite de manera innecesaria la gestión pública o el cumplimiento del mandato institucional.

Compartir el riesgo

Cuando resulte difícil para la entidad reducir el riesgo a un nivel aceptable o se carezca de la capacidad técnica y de los conocimientos necesarios para gestionarlo de manera efectiva, el riesgo podrá ser compartido con otra parte interesada que cuente con mayores recursos o competencias para su administración.

Este tratamiento se materializa, por ejemplo, mediante contratos, convenios, seguros o alianzas estratégicas, que permiten distribuir las consecuencias del riesgo. No obstante, es importante precisar que, aun cuando se comparta, la responsabilidad última frente al riesgo no es transferible y permanece en cabeza de la entidad.

Reducir el riesgo

El tratamiento más habitual consiste en administrar el nivel del riesgo mediante el establecimiento de controles, de tal manera que el riesgo residual se ubique dentro de

los parámetros aceptables definidos por la política institucional de apetito y tolerancia al riesgo.

Estos controles buscan disminuir la probabilidad y/o el impacto de materialización del riesgo, y deberán seleccionarse bajo criterios de eficacia, eficiencia y pertinencia.

Para garantizar su efectividad, se recomienda que los controles:

- Se diseñen conforme a las mejores prácticas técnicas y normativas.
- Incluyan una adecuada segregación de funciones que evite la concentración de responsabilidades.
- Sean objeto de monitoreo y evaluación periódica por parte de las líneas de defensa correspondientes, a fin de verificar su capacidad para lograr la reducción prevista.

Tratamiento del riesgo – rol de la primera línea de defensa

Como medio para propiciar el logro de los objetivos, las actividades de control se orientan a prevenir y detectar la materialización de los riesgos. Por consiguiente, su efectividad depende, de qué tanto se están logrando los objetivos estratégicos y de proceso de la entidad. Le corresponde a la primera línea de defensa el establecimiento de actividades de control.

Ilustración 21. Clasificación de los controles en la gestión de riesgos

Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 6. Pág. 91

4.6 MONITOREO DE RIESGOS DE CORRUPCIÓN

Los Secretarios, Gerentes y Jefes de Oficina, en articulación con sus equipos de trabajo, son responsables de monitorear y revisar de manera periódica la gestión de los riesgos de corrupción, implementando los ajustes necesarios cuando se identifiquen desviaciones, debilidades en los controles o cambios en el contexto (primera línea de defensa).

De manera complementaria, corresponde a la Secretaría Distrital de Planeación adelantar el monitoreo institucional (segunda línea de defensa). Para este propósito se recomienda la utilización de una matriz de seguimiento que consolide la información, facilite la trazabilidad y permita evaluar la efectividad de los controles frente a los riesgos identificados. La periodicidad de este ejercicio será definida por la entidad en coherencia con su planeación institucional y sus instrumentos de gestión.

Este proceso resulta fundamental, dado que la corrupción es un fenómeno de difícil detección y requiere un seguimiento constante, sistemático y documentado que garantice la efectividad de los controles establecidos.

En todo caso, el monitoreo deberá desarrollarse conforme a los lineamientos previstos para la primera y segunda línea de defensa, asegurando la transparencia, la integridad y la rendición de cuentas como principios rectores de la gestión pública.

4.7 REPORTE DE LA GESTIÓN DEL RIESGO DE CORRUPCIÓN

Los riesgos de corrupción deberán ser reportados de manera explícita en el mapa de riesgos y en el plan de tratamiento correspondiente, garantizando que se documente y comunique toda la información necesaria para su comprensión, seguimiento y tratamiento adecuado.

Este reporte constituye una herramienta esencial para:

- Visibilizar los riesgos identificados y su nivel de exposición.
- Integrar las medidas de tratamiento en los planes institucionales de control y gestión.
- Facilitar la trazabilidad y el seguimiento por parte de los órganos de control interno y externo.

- Asegurar que los responsables de proceso cuenten con información oportuna y suficiente para la toma de decisiones.

De esta manera, el reporte no solo fortalece la gestión preventiva frente a riesgos de corrupción, sino que también refuerza los principios de transparencia, integridad y rendición de cuentas que orientan la gestión pública.

4.8 SEGUIMIENTO DE RIESGOS DE CORRUPCIÓN

La Gerencia de Control Interno de Gestión deberá adelantar el seguimiento al mapa de riesgos de corrupción, verificando de manera integral la gestión del riesgo y la efectividad de los controles implementados.

El cronograma de seguimiento será el siguiente:

- **Primer seguimiento:** Con corte al 30 de abril. La publicación del informe deberá realizarse dentro de los diez (10) primeros días del mes de mayo.
- **Segundo seguimiento:** Con corte al 31 de agosto. La publicación del informe deberá realizarse dentro de los diez (10) primeros días del mes de septiembre.
- **Tercer seguimiento:** Con corte al 31 de diciembre. La publicación del informe deberá realizarse dentro de los diez (10) primeros días del mes de enero del año siguiente.

El seguimiento adelantado por la Gerencia de Control Interno de Gestión deberá publicarse en la página web institucional o en un espacio de fácil acceso para la ciudadanía, garantizando la transparencia y la rendición de cuentas (ver Anexo: Matriz de seguimiento a los riesgos de corrupción).

De manera específica, el seguimiento comprenderá las siguientes actividades:

- Verificar la publicación del mapa de riesgos de corrupción en la página web de la entidad.
- Realizar seguimiento a la gestión del riesgo, conforme a los planes de tratamiento establecidos.
- Revisar la evolución de los riesgos y sus niveles de exposición.
- Asegurar que los controles sean efectivos, pertinentes y que estén funcionando de manera adecuada frente a los riesgos identificados.


RIESGOS
SEGURIDAD DE LA
LA INFORMACIÓN

5. LINEAMIENTOS RIESGOS SEGURIDAD DE LA INFORMACIÓN

En el marco de la gestión institucional, se debe tener presente que la Política de Seguridad Digital se articula con el Modelo de Seguridad y Privacidad de la Información (MSPI)[5], el cual se encuentra alineado con el marco de referencia de arquitectura TI.

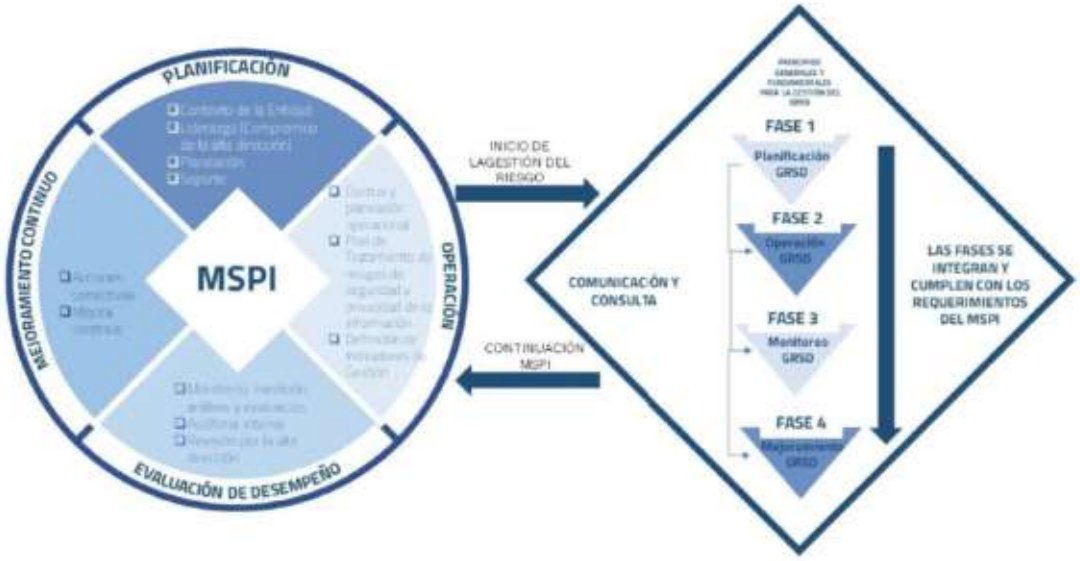
Este modelo constituye un habilitador transversal que soporta de manera integral los demás componentes de la Política de Gobierno Digital, particularmente en lo relacionado con:

- Seguridad de la información.
- Arquitectura empresarial.
- Servicios ciudadanos digitales.

De esta forma, la gestión de los riesgos de seguridad de la información no solo se centra en la protección de los activos tecnológicos e informacionales, sino que también garantiza la confianza digital, la continuidad de los servicios públicos y la protección de los datos de los ciudadanos, en coherencia con los principios de transparencia, integridad y disponibilidad de la información.

[5] El Modelo de Seguridad y Privacidad de la Información - MSPI, imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital. Fuente. Gobierno digital MINTIC.

Ilustración 22. Esquema Integrado del MSPI y el Ciclo de Gestión del Riesgo de Seguridad de la Información (GRSD)



Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas. Anexo 4, MINTIC. 2021. Pág. 8

5.1. IDENTIFICACIÓN DE LOS ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN

Como primer paso en la gestión de los riesgos de seguridad de la información, resulta indispensable identificar los activos de información asociados a cada proceso.

Esta etapa permite reconocer de manera clara cuáles son los activos de tecnología clasificados como críticos que deben ser protegidos, y constituye la base para analizar su nivel de exposición frente a amenazas y vulnerabilidades.

La adecuada identificación y clasificación de estos activos permitirá evaluar su criticidad, establecer prioridades de protección y aplicar controles específicos que garanticen la confidencialidad, integridad y disponibilidad de la información.

Tabla 17. Conceptualización activos de información

¿Qué son los activos?	¿Por qué identificar los activos?
Un activo de información es cualquier elemento que participe en el tratamiento de información que tenga valor para la organización, sin embargo, en el contexto de seguridad de la información son activos elementos tales como: hardware, software, aplicaciones de la entidad, servicios web, redes, información digital,	Permite determinar qué es lo más importante que cada entidad y sus procesos poseen (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios). La entidad puede saber qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su

personal, ubicación, organización, tecnologías de la información – TI o tecnologías de la operación TO, que utiliza la entidad para su funcionamiento y que, por afectación operativa, se afecte el principio de disponibilidad.	funcionamiento de cara al ciudadano, aumentando así su confianza en el uso del entorno digital.

Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas Dirigida a las entidades del Estado Versión 5. Pág. 14

Nota: Para llevar a cabo la identificación de activos de información, se deberá remitirse a la sección 3.1.6 del Anexo 4, "Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas", el cual hace parte integral de los anexos de la presente guía. Este lineamiento asegura la aplicación de un criterio uniforme y estandarizado, en concordancia con las disposiciones nacionales en materia de seguridad digital y gestión de riesgos.

Para realizar la identificación, remitirse a: Lineamientos para el Inventario y Clasificación de Activos de Información e Infraestructura Critica Cibernética Nacional Dirigida a las entidades del Estado, Versión 5.

Ilustración 23. Ejemplo identificación de activos de información

Proceso	Activo	Descripción	Dueño del activo	Tipo del activo	Ley 1712 de 2014	Ley 1581 de 2012	Criticidad respecto a su confidencialidad	Criticidad respecto a su completitud o integridad	Criticidad respecto a su disponibilidad	Nivel de criticidad
Gestión de Recursos Financieros	Base de datos de nómina	Contiene la información de nómina de los servidores y contratistas de la Alcaldía.	Secretaria Distrital de Hacienda	Información	Información reservada	Contiene datos personales sensibles	ALTA	ALTA	ALTA	ALTA
Gestión Humana y SST	Aplicativo de talento humano	Software que administra la información de hojas de vida, procesos de selección y capacitación.	Secretaria Distrital de Gestión Humana	Software	N/A	Contiene datos personales	ALTA	MEDIA	MEDIA	ALTA
Direccionamiento Estratégico y Planeación	Sistema de proyectos	Plataforma que consolida la planeación estratégica y los proyectos de inversión distrital.	Secretaría Distrital de Planeación	Sistema de información	Información pública	No contiene datos personales	MEDIA	ALTA	ALTA	ALTA
Gestión del Servicio Educativo	Base de datos de matrícula	Información de estudiantes, sedes y niveles educativos de la ciudad.	Secretaría Distrital de Educación	Información	Información pública	Contiene datos personales	ALTA	ALTA	ALTA	ALTA
Gestión de la salud	Registro de atención en salud	Historias clínicas y reportes epidemiológicos de la red distrital.	Secretaría Distrital de Salud	Información	Información reservada	Contiene datos sensibles	ALTA	ALTA	MEDIA	ALTA
Atención al Ciudadano	Ventanilla Única Distrital	Aplicativo que gestiona trámites y servicios solicitados por los ciudadanos.	Oficina de Relación con el Ciudadano	Software	Información pública	Contiene datos personales	ALTA	MEDIA	ALTA	ALTA

Construcción propia

5.2 IDENTIFICACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

En el marco de la gestión institucional, se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

- Pérdida de la confidencialidad: acceso no autorizado a la información.
- Pérdida de la integridad: alteración no autorizada de la información o de los sistemas que la procesan.
- Pérdida de la disponibilidad: indisponibilidad de los sistemas o datos cuando son requeridos para la operación institucional.

Para cada riesgo, deberá asociarse el grupo de activos o los activos específicos del proceso, y analizar de manera conjunta las posibles amenazas y vulnerabilidades que podrían ocasionar su materialización.

Con este propósito, se debe consultar el Anexo 4: Modelo Nacional de Gestión de Riesgos de Seguridad de la Información para Entidades Públicas, en el cual se encuentran las tablas de referencia necesarias para el análisis:

- Tabla de amenazas comunes.
- Tabla de amenazas dirigida por el hombre.
- Tabla de vulnerabilidades comunes.

📌*Nota: La sola existencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o de un control. Para que la vulnerabilidad se materialice, es necesario que una amenaza la explote. Por lo tanto, una vulnerabilidad sin amenaza asociada puede no requerir la implementación inmediata de un control.*

Tabla 18. Tabla de amenazas y vulnerabilidades de acuerdo con el tipo de activo

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Almacenamiento de medios sin protección	Hurto de medios o documentos
Software	Ausencia de parches de seguridad	Abuso de los derechos
Red	Líneas de comunicación sin protección	Escucha encubierta
Información	Falta de controles de acceso físico	Hurto de información
Personal	Falta de capacitación en las herramientas	Error en el uso
Organización	Ausencia de políticas de seguridad	Abuso de los derechos

Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 6. Pág. 98

En la siguiente tabla se observa un ejemplo de identificación del riesgo sobre un activo como es la base de datos de nómina:

Tabla 19. Formato de descripción del riesgo de seguridad de la información

RIESGO	ACTIVO	DESCRIPCIÓN DEL RIESGO	AMENAZA	TIPO	CAUSA VULNERABILIDADES*	CONSECUENCIA
Base de datos de nómina	Pérdida de la integridad	La falta de políticas de seguridad digital, ausencia de políticas de control de acceso, contraseñas sin protección y mecanismos de autenticación débil, pueden facilitar una modificación no autorizada, lo cual causaría la pérdida de la integridad de la base de datos de nómina	Modificación no autorizada	Seguridad digital	- Falta de políticas de seguridad digital - Ausencia de políticas de control de acceso - Contraseñas sin protección - Autenticación débil	Posibles consecuencias que puede enfrentar la entidad o el proceso a causa de la materialización del riesgo (legales, económicas, sociales, reputacionales, confianza en el ciudadano). Ejemplo: posible retraso en el pago de nómina

*Seleccionar las vulnerabilidades asociadas a la amenaza identificada

- Existirán tres (3) tipos de riesgos: pérdida de confidencialidad, pérdida de la integridad y pérdida de la disponibilidad de los activos. Para cada tipo de riesgo se podrán seleccionar las amenazas y las vulnerabilidades que puedan causar que dicho riesgo se materialice.
- Los catálogos de amenazas y vulnerabilidades comunes se encuentran en el Anexo 4: Modelo Nacional de Gestión de Riesgos de Seguridad de la Información para Entidades Públicas.

📌*Nota: La agrupación de activos deberá realizarse siempre por categorías homogéneas. En este sentido, resulta pertinente analizar de manera conjunta los activos de tipo hardware, software, información, red o personal, con el propósito de identificar las amenazas y vulnerabilidades comunes que puedan incidir en dicho grupo y afectar la gestión institucional.*

5.3 VALORACIÓN DEL RIESGO

Para esta etapa, se deberán asociar las tablas de probabilidad e impacto definidas en la primera parte de la presente guía, con el fin de valorar de manera integral los riesgos identificados.

En este sentido, deberá considerarse específicamente la **Tabla 4. Criterios para definir el nivel de probabilidad**, establecida en el aparte 3.2.1, como referencia metodológica para la calificación del nivel de probabilidad e impacto de cada riesgo, garantizando así uniformidad en el análisis y coherencia con el modelo de gestión adoptado por la entidad.

La determinación del impacto se debe llevar a cabo de acuerdo con lo establecido en el aparte 3.2.2 de la presente guía, entendiendo que el impacto se entiende como la consecuencia económica y reputacional que se genera por la materialización del riesgo. En este sentido, se debe considerar para este análisis la **Tabla 5. Criterios para definir el nivel de impacto.**

Para el análisis preliminar (riesgo inherente), en esta etapa se define el nivel de severidad para el riesgo de seguridad de la información identificado, para ello, se aplica la matriz de calor establecida en el numeral 3.2.2 de la presente guía, que se retoma a continuación. Este análisis preliminar permite determinar el riesgo inherente, es decir, el nivel de exposición al que estaría sujeta la entidad antes de considerar la aplicación de controles, y constituye la base para priorizar las acciones de tratamiento.

Nota: Las variables de confidencialidad, integridad y disponibilidad se definen conforme al Modelo de Seguridad y Privacidad de la Información (MSPI), en el marco de la Estrategia de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones.

Riesgo	Activo	Amenaza	Vulnerabilidad	Probabilidad	Impacto	Zona de Riesgo
Perdida de Confidencialidad	Base de datos nomina	Modifica no autorizada	Ausencia de políticas de control de acceso	4- Probable	4-Mayor	Extrema
			Contraseña sin protección			
			Ausencia de mecanismos de identificación autenticación de usuarios			
			Ausencia de bloqueo de sesión			

Nota: La probabilidad y el impacto se determinan con base a la amenaza, no a las vulnerabilidades.

5.4 CONTROLES ASOCIADOS A LA SEGURIDAD DE LA INFORMACIÓN

La entidad deberá mitigar y tratar los riesgos de seguridad de la información empleando, como mínimo, los controles establecidos en el Anexo A de la norma ISO/IEC 27001:2013, los cuales se encuentran recopilados en el Anexo 4: Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas. Estos controles deberán seleccionarse de manera coherente con los resultados del análisis de riesgos institucional, asegurando su pertinencia y eficacia.

De acuerdo con el control definido, será necesario considerar las características de diseño y de ejecución establecidas para su correcta valoración, con el fin de garantizar que el tratamiento aplicado contribuya al fortalecimiento de la confidencialidad, integridad y disponibilidad de la información.

A manera de referencia, se incluyen algunos ejemplos de controles y sus dominios asociados. La lista completa se encuentra en el documento maestro del Modelo de Seguridad y Privacidad de la Información (MSPI), que constituye el marco orientador para la adopción de controles en las entidades públicas.

Tabla 20. Controles para riesgos de seguridad de la información

Area de control	Aplicación en la entidad
Procedimientos de operación documentados	Los procedimientos de operación deben estar documentados y disponibles para las dependencias que gestionan sistemas críticos (ej. nómina, sistemas tributarios, recaudos, inventarios), garantizando su uso uniforme y trazable.
Gestión de cambios	Todo cambio en sistemas institucionales (SIIF, SECOP II, plataformas internas financieras, contables entre otras) deberá ser controlado y registrado para evitar alteraciones no autorizadas que afecten la seguridad digital o la continuidad de los servicios ciudadanos.
Gestión de capacidad	Se debe dar seguimiento al uso de recursos tecnológicos (servidores, almacenamiento, red) de los sistemas institucionales, con proyecciones de capacidad que permitan garantizar la atención de picos de demanda (ej. matrícula escolar, recaudo tributario).
Separación de ambientes de desarrollo, pruebas y operación	Los desarrollos de software interno y las actualizaciones de sistemas contratados deberán gestionarse en ambientes separados, evitando que cambios no autorizados impacten los servicios de atención al ciudadano.
Protección contra códigos maliciosos	Los equipos y sistemas institucionales deberán contar con medidas de protección (antivirus, filtros de correo, firewall) para garantizar que los activos de información de la Alcaldía estén protegidos contra malware y ciberataques.
Controles contra códigos maliciosos	La Gerencia de Tecnología de la Información y Comunicaciones – TIC, deberá implementar controles de detección, prevención y recuperación, acompañados de campañas de concienciación a funcionarios y contratistas sobre el uso seguro de la información y protección frente a ataques.
Copias de respaldo	Se deberán establecer políticas de respaldo que protejan los datos institucionales contra pérdida, incluyendo copias de seguridad de bases de datos críticas (nómina, matrícula, recaudo).
Respaldo de información	Las copias de respaldo de información, software y configuraciones de sistemas deberán almacenarse en medios seguros y probarse periódicamente, de acuerdo con las políticas de continuidad de negocio de la Alcaldía.

Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 6. Pág. 104

Tabla 21. Formato mapa riesgos seguridad de la información

N.	RIESGO	ACTIVO	TIPO	AMENAZAS	TIPO	PROBABILIDAD	IMPACTO	RIESGO RESIDUAL	OPCIÓN TRATAMIENTO	ACTIVIDAD DE CONTROL	SOPORTE	RESPONSABLE	TIEMPO	INDICADOR
2	**Pérdida de la integridad**	Base de datos de nómina	Seguridad digital	Modificación no autorizada	Ausencia de políticas de control de acceso	**Probable**	**Menor**	**Moderado**	Reducir	A.9.1.1 Política de control de acceso	Política creada y comunicada	Oficina TI	Tercer trimestre de 2018	**EFICACIA:** Índice de cumplimiento actividades= (# de actividades cumplidas / # de actividades programadas) x 100 **EFECTIVIDAD:** Efectividad del plan de manejo de riesgos= (# de modificaciones no autorizadas)
					Contraseñas sin protección				Reducir	A.9.4.3 Sistema de gestión de contraseñas	Procedimientos para la gestión y protección de contraseñas	Oficina TI	Tercer trimestre de 2018	
					Ausencia de mecanismos de identificación y autenticación de usuarios				Reducir	A 9.4.2 Procedimiento de ingreso seguro	Procedimiento para ingreso seguro	Oficina TI	Tercer trimestre de 2018	
					"Ausencia de bloqueo				Reducir	A.11.2.8 Equipos de usuario desatendidos	Configuraciones para bloqueo automático de sesión	Oficina TI	Tercer trimestre de 2018	

Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 6. Pág. 105


RIESGOS
FISCALES

6. LINEAMIENTOS RIESGOS FISCALES

6.1 CONTROL FISCAL INTERNO Y PREVENCIÓN DEL RIESGO FISCAL

La construcción de este capítulo se erige sobre la premisa fundamental de la responsabilidad fiscal, cuyo núcleo esencial es la prevención del daño al patrimonio público. Este daño, conforme al Decreto 403 de 2020[6] (artículo 6), se manifiesta en el menoscabo, la disminución, el perjuicio, el detrimento, la pérdida o el deterioro de los bienes y recursos públicos, así como de los intereses patrimoniales del Estado.

En el caso particular de la Alcaldía Distrital de Barranquilla, este enfoque cobra una relevancia especial en la medida en que la ciudad, como Distrito Especial, Industrial y Portuario, gestiona importantes recursos en materia de, educación, salud, infraestructura, programas sociales, ambientales y de desarrollo económico. Proteger el patrimonio público en este contexto no solo garantiza la sostenibilidad de las finanzas distritales, sino que fortalece la confianza ciudadana en la gestión pública y en la construcción de valor colectivo.

Las bases normativas que regulan la responsabilidad fiscal en Colombia se encuentran en la Ley 610 de 2000[7], y su marco constitucional en los artículos 267 y 268 de la Constitución Política de 1991, modificados por el Acto Legislativo 04 de 2019[8]. Este último fortaleció el carácter preventivo del control fiscal, introduciendo la necesidad de identificar tempranamente los riesgos fiscales para detener la materialización del daño y habilitar al gestor público para adoptar medidas correctivas y de mitigación oportunas.

En este contexto, el control fiscal dejó de ser exclusivamente posterior y selectivo —tradicionalmente materializado a través de auditorías y ejercicios de control micro[9]—, para transformarse en un sistema preventivo, concomitante y multinivel, orientado al ejercicio permanente de vigilancia sobre los recursos públicos. Una de sus herramientas más significativas es la articulación con el Sistema de Control Interno, lo que da origen a dos conceptos cardinales:

---

[6] Por el cual se dictan normas para la correcta implementación del Acto Legislativo 04 de 2019 y el fortalecimiento del control fiscal

[7] por la cual se establece el trámite de los procesos de responsabilidad fiscal de competencia de las contralorías.

[8] Por medio del cual se reforma el Régimen de Control Fiscal

[9] Vigilancia de la gestión fiscal de cada una de las entidades que conforman la estructura administrativa del Estado y de las personas privadas que manejen fondos o bienes del Estado.

- **Control Fiscal Multinivel:** Articulación entre el Sistema de Control Interno (primer nivel de control), el Control Externo (segundo nivel de control, ejercido por las contralorías) y el Control Social, entendido como la participación de la ciudadanía en la vigilancia de los recursos públicos. Este enfoque amplía el espectro de protección patrimonial y democratiza el ejercicio del control.

- **Control Fiscal Interno (CFI):** Representa el primer nivel de vigilancia fiscal sobre los recursos públicos y constituye un mecanismo esencial de prevención de riesgos fiscales y defensa del patrimonio. Hace parte del Sistema de Control Interno, por lo que es responsabilidad compartida de todos los servidores públicos y de los particulares que administran recursos, bienes e intereses patrimoniales de naturaleza pública. Su efectividad es evaluada por la Contraloría respectiva, y dicha evaluación resulta determinante para el fenecimiento de la cuenta, esto es, la aprobación o no aprobación de la gestión fiscal adelantada.

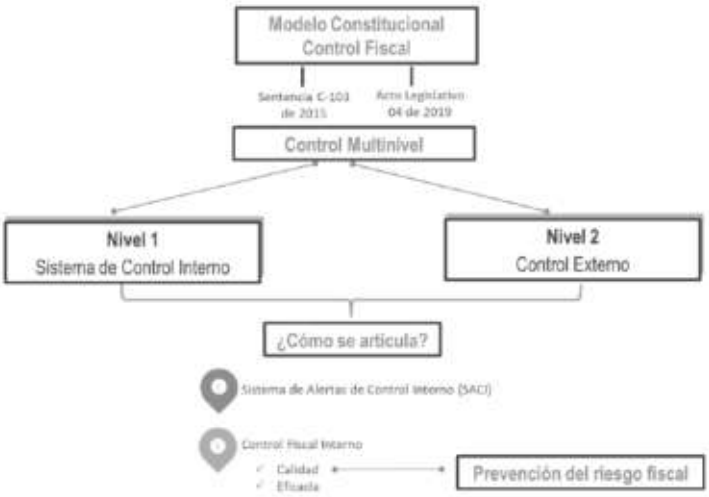
En el nuevo modelo constitucional, el Control Externo adquiere una dimensión preventiva, mientras que el Control Interno refuerza este enfoque, partiendo de la premisa de que el Sistema de Control Interno es un eje estratégico para conjugar dos propósitos:

1. El logro de resultados institucionales en concordancia con los objetivos misionales de la Alcaldía Distrital de Barranquilla.

2. La prevención de riesgos de gestión, corrupción y fiscales, así como la protección del gestor público —jefes de entidad, ordenadores y ejecutores del gasto, pagadores, estructuradores de contratos, responsables de planeación contractual, supervisores y responsables de labores de cobro—, al evitar la configuración de responsabilidades administrativas, disciplinarias o fiscales.

La siguiente figura muestra este despliegue y sus elementos de articulación que sustentan el desarrollo del presente capítulo.

Ilustración 24. Articulación modelo constitucional control fiscal y sistema de control interno



Elaboración Dirección de Gestión y Desempeño Institucional de Función Pública, 2022

El paso a paso de la gestión del riesgo fiscal: identificación, análisis y valoración, debe integrarse al análisis general de riesgos institucionales. El propósito de esta integración es consolidar un esquema integral de administración de riesgos que facilite el seguimiento sistemático por parte de los líderes de proceso, asegurando trazabilidad y rendición de cuentas.

La metodología propuesta se fundamenta en buenas prácticas internacionales, como la ISO 31000:2018 y el marco COSO ERM, y se orienta a gestionar de manera efectiva los recursos, bienes e intereses públicos, reduciendo la probabilidad de materialización de daños fiscales y mitigando la configuración de responsabilidades fiscales.

Como insumo adicional, se incorpora un Catálogo Indicativo y Enunciativo de Puntos de Riesgo Fiscal y Circunstancias Inmediatas (ver anexo). El catálogo constituye un marco de referencia invaluable para identificar y valorar riesgos fiscales, ofreciendo un compendio de tipologías de riesgo sustentadas en precedentes.

No obstante, la entidad debe realizar un ejercicio autónomo y contextualizado, ajustando los puntos de riesgo y circunstancias inmediatas allí consignadas a sus propias realidades. Es decir, cada secretaría, gerencia u oficina deberá considerar su naturaleza, complejidad, portafolio de productos y servicios, usuarios o grupos de valor, recursos disponibles, entorno sectorial y demás condiciones específicas.

6.2 DEFINICIÓN Y ELEMENTOS DEL RIESGO FISCAL

Teniendo en cuenta la estructura y elementos de la definición de riesgos que tiene la presente guía, la cual es armónica con la norma ISO 31000, se define riesgo fiscal, así:

> Efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un **evento potencial**

A continuación, se describen los elementos que conforman la definición de riesgo fiscal:

- **Efecto:** es el daño que se generaría sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, en caso de ocurrir el evento potencial.
- **Evento Potencial:** hechos inciertos o incertidumbres, refiriéndonos a riesgo fiscal, se relaciona con una potencial acción u omisión que podría generar daño sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública. En esta guía, el evento potencial es equivalente a la causa raíz.

Lo anterior se puede resumir de la siguiente manera:

> **Riesgo Fiscal =** Evento Potencial (Potencial Conducta) **+** Efecto dañoso

📌*Nota: Se debe tener especial cuidado en no confundir el riesgo fiscal, con el daño fiscal; por lo tanto, la definición debe estar orientada hacia el efecto de un evento potencial (potencial acción u omisión) sobre los recursos públicos y/o los bienes o intereses patrimoniales de naturaleza pública.*

A continuación, se presenta la metodología y el paso a paso que orienta la identificación, clasificación, valoración y control de los riesgos fiscales. Este procedimiento constituye un insumo esencial para el fortalecimiento de la gestión institucional y para la garantía de la seguridad y la prevención de responsabilidades fiscales de los gestores públicos.

El proceso está dirigido a todos los actores involucrados en la administración y ejecución de recursos públicos, incluyendo secretarios, gerentes, ordenadores y ejecutores del gasto, pagadores, funcionarios responsables de la estructuración y de la planeación contractual, supervisores y encargados de labores de cobro, entre otros.

6.3 IDENTIFICACIÓN DE RIESGOS FISCALES

6.3.1 PUNTOS DE RIESGO FISCAL Y CIRCUNSTANCIAS INMEDIATAS

Para la identificación del riesgo fiscal es indispensable establecer los puntos de riesgo fiscal y las circunstancias inmediatas.

- **Puntos de riesgo fiscal:** son aquellas situaciones en las que potencialmente se puede generar un riesgo fiscal. Corresponden a las actividades relacionadas con la administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de bienes o recursos públicos, así como a la recaudación, manejo e inversión de rentas. En conclusión, los puntos de riesgo fiscal comprenden todas las actividades que representen gestión fiscal, incluyendo aquellas en las cuales se han presentado advertencias, alertas, hallazgos fiscales o fallos con responsabilidad fiscal.

- **Circunstancias inmediatas:** son las situaciones bajo las cuales se presenta el riesgo fiscal, sin constituir la causa principal o raíz. Es importante resaltar que, para un mismo punto de riesgo fiscal, pueden existir múltiples circunstancias inmediatas que deben analizarse en detalle.

Para identificar los puntos de riesgo y las circunstancias inmediatas de manera rigurosa, se recomienda realizar un taller con la participación de directivos, asesores y servidores públicos que, por su conocimiento, experiencia o formación, puedan aportar valor en el análisis. Como apoyo metodológico, este taller puede guiarse con preguntas orientadoras que faciliten la reflexión, el debate y la identificación estructurada de riesgos, asegurando un análisis integral y ajustado al contexto de la Alcaldía Distrital de Barranquilla.

Tabla 22. Preguntas orientadoras para puntos riesgo fiscal y causas inmediatas

Sirve para identificar	Preguntas orientadoras	Respuestas esperadas / Fuente de información	Notas / Consideraciones
Puntos de riesgo fiscal	¿En qué procesos de la entidad se realiza gestión fiscal? (ver capítulo inicial la definición de gestión fiscal).	Procesos estratégicos, misionales, de apoyo y de avaluación donde se administren, recauden, inviertan o dispongan recursos públicos.	Se debe usar el mapa de procesos de la entidad como referencia.
Puntos de riesgo fiscal y circunstancias inmediatas	Clasifique por procesos (según el mapa de procesos de la entidad) los hallazgos con presunta incidencia fiscal, fallos con responsabilidad fiscal en	Listado de hallazgos, fallos y advertencias, organizados por procesos.	Nota 1: Revisar hallazgos con presunta incidencia fiscal y los fallos con responsabilidad fiscal de los últimos 5 años.

	firme, advertencias de la CGR y alertas reportadas en el Sistema de Alertas de Control Interno – SACI.		Nota 2: Consultar la matriz de plan de mejoramiento institucional y los históricos de la Gerencia de Control Interno de Gestión. Nota 3: La organización de los hallazgos, fallos, advertencias de la CGR y alertas reportadas corresponde a la segunda línea de defensa: Secretaría Distrital de Planeación, con asesoría de la Gerencia de Control Interno de Gestión.
Circunstancias inmediatas	En un ejercicio autocrítico, realista y objetivo: ¿Cuáles son las causas de los hallazgos fiscales identificados, fallos con responsabilidad fiscal, advertencias de la OCI o de la CGR, en los últimos 3 años?	Descripción de causas inmediatas, diferenciando entre situaciones evidentes y causas raíz.	Nota 1: Se recomienda no copiar literalmente las causas escritas por los órganos de control, salvo que luego del análisis interno se confirme que corresponden a la causa real.
Puntos de riesgo fiscal y circunstancias inmediatas	¿Qué puntos de riesgo fiscal y circunstancias inmediatas del "Catálogo Indicativo y Enunciativo de Puntos de Riesgo Fiscal y Circunstancias Inmediatas" aplican a la entidad?	Listado de puntos y circunstancias aplicables, contextualizados al sector y a la entidad.	Este catálogo es un insumo de referencia que debe adaptarse al contexto de la Alcaldía Distrital de Barranquilla.

Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 6. Pág. 70-71

6.3.2 IDENTIFICACIÓN DE ÁREAS DE IMPACTO

En el contexto del riesgo fiscal, el área de impacto se entiende siempre como una consecuencia económica sobre el patrimonio público, a la cual se ve expuesta la entidad en caso de materializarse un riesgo. Esta aproximación permite distinguir de manera precisa cuándo un evento constituye realmente un riesgo fiscal y cuándo se trata de un efecto económico de otra naturaleza.

Es fundamental señalar que no todos los efectos económicos constituyen riesgos fiscales, aunque todo riesgo fiscal sí representa necesariamente un efecto económico sobre bienes, recursos o intereses patrimoniales de naturaleza pública.

📌*Nota: Ejemplos de efectos económicos que no son riesgos fiscales:*

1. *Riesgo de daño antijurídico: asociado al pago de condenas judiciales o conciliaciones, que, si bien generan un impacto económico, no corresponden a un riesgo fiscal en sentido estricto.*
2. *Efectos económicos derivados de causas exógenas: aquellos que no tienen relación con la acción u omisión de los gestores públicos, tales como casos de*

fuerza mayor, hechos fortuitos o actos de un tercero (que no ostente la calidad de gestor público).

Por lo tanto, al momento de identificar y redactar un riesgo fiscal, es imprescindible delimitar claramente el impacto económico real y vincularlo únicamente a los eventos que efectivamente configuren riesgo fiscal.

Otro aspecto clave para esta definición es la comprensión del concepto de patrimonio público y de las tres expresiones que lo integran, de acuerdo con lo establecido en el artículo 6 de la Ley 610 de 2000:

- Bienes públicos.
- Recursos públicos.
- Intereses patrimoniales de naturaleza pública.

6.3.3 IDENTIFICACIÓN DE LA CAUSA RAÍZ O POTENCIAL HECHO GENERADOR

La causa raíz corresponde a cualquier evento potencial —acción u omisión— que, de materializarse, podría generar un menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro del patrimonio público (Auditoría General de la República, 2015).

Existe, por tanto, una relación directa de causa/efecto entre la causa raíz o potencial hecho generador y el efecto dañoso o daño fiscal. En este sentido, la determinación de la causa raíz implica establecer con precisión la acción u omisión específica que, de presentarse, ocasionaría el acto lesivo al patrimonio estatal.

Es fundamental destacar que, por su relevancia, la causa raíz debe diferenciarse claramente del daño:

- **Hecho generador – Causa raíz o causa adecuada:** es el evento o situación (acción u omisión) que origina el riesgo fiscal.

- **Daño – Efecto:** es la consecuencia económica derivada del hecho generador, expresada en pérdida, detrimento o deterioro de los recursos públicos (Contraloría General de la República, 2021).

En conclusión, uno es el hecho que genera el daño (causa raíz), y otro es el daño mismo (efecto). Esta distinción es determinante para orientar la política de control fiscal de la Alcaldía Distrital de Barranquilla, asegurando que las acciones de prevención se

concentren en neutralizar los hechos generadores que podrían comprometer el patrimonio público.

Tabla 23. Ejemplos de Identificación de daño fiscal y hecho generador

Situación	Daño Fiscal	Hecho Generador (Causa raíz)	Conclusión
1. Canon de arrendamiento: Una entidad X se atrasó en el pago del canon de arriendo de una de sus sedes por 6 meses, generándose intereses moratorios por $30 millones. Cuando llega un nuevo director, encuentra la deuda y gestiona los recursos, efectuando el pago de capital e intereses al mes de su posesión.	Corresponde al monto pagado por concepto de intereses moratorios ($30 millones).	Omisión en el pago oportuno del canon de arrendamiento.	El hecho generador del daño no es el pago de los intereses, ya que este fue un acto diligente para cumplir con la obligación y frenar más intereses. El daño se origina en la omisión inicial de pago oportuno.
2. Contratación pública: Una entidad adjudica un contrato de obra sin verificar la idoneidad técnica y financiera del contratista. Este incumple parcialmente, dejando la obra inconclusa y obligando a la entidad a pagar $500 millones adicionales para finalizarla con otro contratista.	El valor adicional pagado por la entidad para finalizar la obra con un nuevo contratista ($500 millones).	Falta de verificación de requisitos e idoneidad del contratista en la etapa de adjudicación.	El daño no está en contratar a un nuevo proveedor, sino en la omisión inicial de verificar la capacidad del contratista, que generó un mayor gasto para la entidad.
3. Manejo presupuestal: Una entidad no apropia en su presupuesto anual el valor estimado de impuestos prediales de un bien de su propiedad. Al no pagar dentro del plazo legal, se generan sanciones e intereses por $80 millones.	Pago por sanciones e intereses tributarios ($80 millones).	Omisión en la programación y pago oportuno de impuestos en el marco de la planeación presupuestal.	El hecho generador no es el pago de la sanción, sino la falta de planeación y gestión presupuestal que impidió cumplir con la obligación a tiempo.

Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 6. Pág. 72

6.3.4 DESCRIPCIÓN DEL RIESGO FISCAL

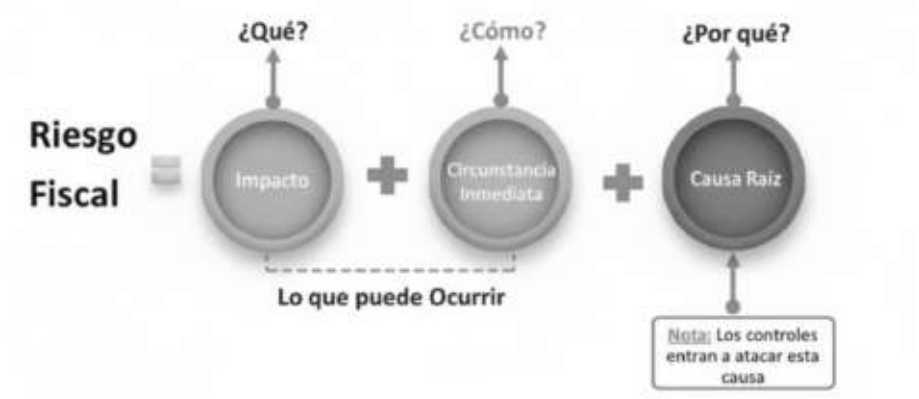
A continuación, se presenta la estructura de redacción de riesgos fiscales en la que se conjugan los elementos antes descritos; así mismo, se presentan algunos ejemplos de riesgos fiscales identificados como resultado del estudio de fallos de contralorías territoriales y Contraloría General de la República.

Para redactar un riesgo fiscal se debe tener en cuenta la siguiente estructura:

1. Inicio: "Posibilidad de", dado que el riesgo se refiere a un evento potencial.
2. Impacto (¿Qué?): Se refiere al efecto dañoso (potencial daño fiscal) sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública (área de impacto).

3. Circunstancia inmediata (¿Cómo?): Se refiere a aquella situación por la que se presenta el riesgo; pero no constituye la causa principal o básica -causa raíz- para que se presente el riesgo.

4. Causa raíz (¿Por qué?): Es el evento (acción u omisión) que de presentarse es causante, es decir, generador directo, causa eficiente o adecuada. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se genera.



Ejemplo de Riesgo Fiscal

Proceso: Gestión de Recursos

Objetivo: Gestionar los bienes, obras y servicios administrativos, de mantenimiento y asistencia logística para el cumplimiento de la misión institucional.

Alcance: Desde la consolidación y depuración del plan de necesidades de bienes, obras y servicios requeridos en cada vigencia fiscal hasta el suministro de bienes y la prestación de servicios, de acuerdo con la disponibilidad de recursos.

¿Qué?	¿Cómo?	¿Por qué?
Posibilidad de efectos dañoso sobre **bienes públicos**	por pérdida, extravío o hurto de bienes muebles de la entidad.	a causa de la omisión en la aplicación del procedimiento para el ingreso y salida de bienes del almacén

Como complemento a continuación se muestran otros ejemplos de redacción de riesgos fiscales, según el objeto sobre el cual recae la posibilidad de efecto dañoso, es decir efecto dañoso sobre bienes públicos, recursos públicos o sobre intereses patrimoniales de naturaleza pública.

Tabla 24. Ejemplos adicionales acorde con el objeto sobre el que recae el efecto dañoso

Objeto sobre el que cae el efecto dañoso	Ejemplo de redacción del riesgo fiscal
Bienes públicos	Posibilidad de efecto dañoso sobre bienes públicos, por daño en equipos tecnológicos, a causa de la omisión en la aplicación de medidas de prevención frente a posibles sobrecargas eléctricas.
Recursos públicos	Posibilidad de efecto dañoso sobre los recursos públicos, por pago de multa impuesta por la autoridad ambiental, a causa de la omisión en el cumplimiento de la licencia ambiental de los proyectos de infraestructura.
Intereses patrimoniales de naturaleza pública	Posibilidad de efecto dañoso sobre intereses patrimoniales de naturaleza pública, por no tener incluidos todos los bienes muebles e inmuebles de la entidad en el contrato de seguro, a causa de la omisión en la actualización de bienes que cubre dicho contrato.
Recursos públicos	Posibilidad de efecto dañoso sobre los recursos públicos, por sobrecostos en contratos de la entidad, a causa de la omisión del deber de elaborar estudios de mercado.
Intereses patrimoniales de naturaleza pública	Posibilidad de efecto dañoso sobre intereses patrimoniales de naturaleza pública, por no devolución al tesoro público de los rendimientos financieros generados por recursos de anticipo, a causa de la omisión por parte de la interventoría y/o supervisión de la interventoría al no exigir la devolución al contratista.

Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 6. Pág. 74

6.4 VALORACIÓN DEL RIESGO FISCAL

6.4.1 EVALUACIÓN DE RIESGOS

Se busca establecer la probabilidad inherente de ocurrencia del riesgo fiscal y sus consecuencias o impacto inherentes.

DETERMINAR LA PROBABILIDAD

La probabilidad es la posibilidad de ocurrencia del riesgo fiscal, se determina según al número de veces que se pasa por el punto de riesgo fiscal en el periodo de 1 año, es decir, el número de veces que se realizan las actividades que representen gestión fiscal.

El nivel de probabilidad de definirá atendiendo los parámetros del numeral 3.2.1 de la presente guia.

DETERMINAR EL IMPACTO

Considerando la naturaleza y alcance del riesgo fiscal, este siempre conlleva un impacto económico, en tanto que el efecto dañoso recae necesariamente sobre un bien, recurso o interés patrimonial de naturaleza pública.

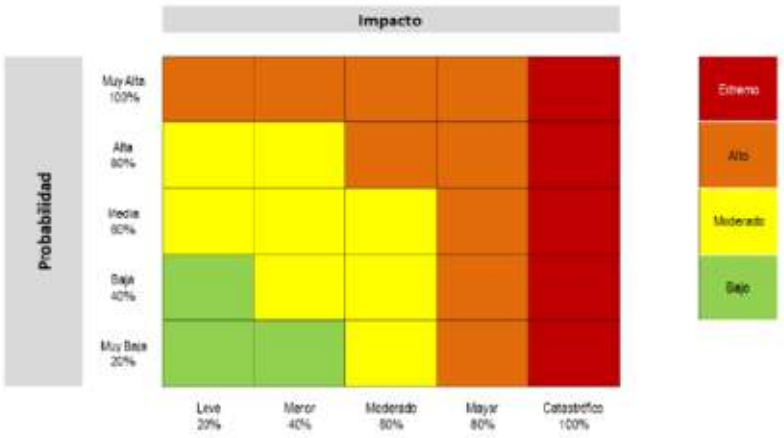
Toda consecuencia económica potencial sobre el patrimonio público resulta relevante para la adecuada gestión fiscal y la prevención de riesgos fiscales.

En coherencia con lo anterior, y para efectos de estandarizar el análisis institucional, se aplicará la tabla de niveles de impacto definida en el numeral 3.2.1 de la presente guía.

6.4.2 DETERMINACIÓN DEL NIVEL DE RIESGO INHERENTE

A partir del análisis de la probabilidad de ocurrencia del riesgo y de sus consecuencias o impacto, se busca determinar la zona de riesgo inicial, también denominada riesgo inherente. Este corresponde al nivel de exposición al que se encuentra la entidad antes de considerar la existencia de controles.

Para este fin, se aplicará la matriz de probabilidad e impacto definida en el numeral 3.2.2 de la presente guía, la cual permite ubicar cada riesgo identificado en una zona de riesgo (bajo, moderado, alto o extremo), según la combinación de estas dos variables.



Nota: **Ejemplo (continuación):**

Proceso: Gestión de Recursos

Objetivo: Gestionar los bienes, obras y servicios administrativos, de mantenimiento y asistencia logística para el cumplimiento de la misión institucional

Alcance: Inicia con la consolidación y depuración del plan de necesidades de bienes, obras y servicios que requieran los procesos institucionales en cada vigencia fiscal y culmina con el suministro de bienes y la prestación de los servicios, acorde con la disponibilidad de recursos

Punto de Riesgo: Ingreso, custodia y salida de bienes muebles de la entidad

Riesgo Fiscal: Posibilidad de efecto dañoso sobre bienes públicos (área de impacto), por pérdida, extravío o hurto de bienes muebles de la entidad (circunstancia inmediata), a causa de la omisión en la aplicación del procedimiento para el ingreso, custodia y salida de bienes del almacén (causa raíz)"

Probabilidad:

El punto de riesgo se enfrenta diariamente, dado que la custodia de los bienes muebles de la entidad se ejerce los 365 días del año.

Aplicando las tablas de probabilidad e impacto tenemos:

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad se realiza máximo 4 veces por año.	20%
Baja	La actividad se realiza mínimo 5 veces al año y máximo 12 veces al año.	40%
Moderada	La actividad se realiza mínimo 13 veces al año y máximo 365 veces al año.	60%
Alta	La actividad se realiza mínimo 365 veces al año y máximo 3660 veces al año.	80%
Muy Alta	La actividad se realiza 3661 veces o más al año.	100%

La actividad se realiza 365 veces al año, la probabilidad de ocurrencia del riesgo es **media**.

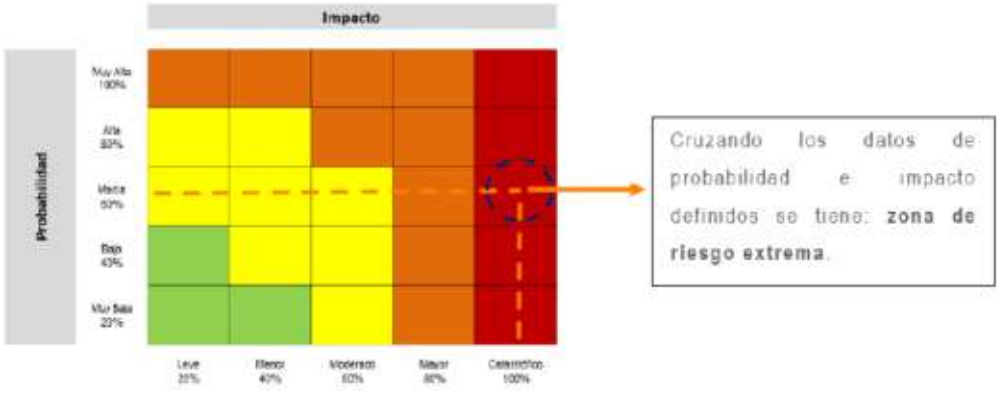
La afectación económica se calcula en más de 500SMLMV, el impacto del riesgo es **catastrófico**.

Para determinar el impacto de un riesgo fiscal es indispensable cuantificar el potencial efecto dañoso sobre el bien, recurso o interés patrimonial de naturaleza pública comprometido. En el ejemplo analizado, el efecto dañoso corresponde al valor contable del inventario de bienes muebles, el cual asciende a $2.500 millones de pesos, equivalentes a 2.500 SMLMV. Con base en la tabla de niveles de impacto definida en la guía, este valor ubica el riesgo en un nivel de impacto catastrófico.

Impacto inherente: catastrófico 100%

De acuerdo con la tabla de definición de zonas de severidad, al combinar la calificación de probabilidad con la de impacto obtenida en el análisis, este riesgo se ubica en un nivel de riesgo extremo.

Este resultado evidencia una exposición crítica para la entidad, lo que exige la implementación inmediata de controles robustos y eficaces, así como un seguimiento prioritario por parte de los responsables del proceso y de las líneas de defensa institucionales, en concordancia con la Política de Administración de Riesgos de la Alcaldía Distrital de Barranquilla.



6.5 VALORACIÓN DE CONTROLES

Como medio para propiciar el logro de los objetivos institucionales, las actividades de control se orientan a prevenir, detectar y corregir la posible materialización de los riesgos fiscales. Estos controles actúan en diferentes momentos del proceso y se clasifican de la siguiente manera:

- Control preventivo: se activa en la entrada del proceso, antes de que se ejecute la actividad en la cual potencialmente se origina el riesgo fiscal (punto de riesgo). Su propósito es establecer condiciones que permitan atacar la causa raíz y evitar que el riesgo se concrete.

- Control detectivo: se aplica durante la ejecución de la actividad en la que se origina el riesgo fiscal. Estos controles permiten identificar oportunamente la ocurrencia de desviaciones, aunque generan la necesidad de reprocesos para subsanar las irregularidades detectadas.

- Control correctivo: se acciona en la salida del proceso y una vez el riesgo se ha materializado. Su objetivo es corregir los efectos y mitigar las consecuencias del daño fiscal, aunque conllevan costos implícitos para la entidad.

Para el análisis y evaluación de los controles diseñados, deben considerarse atributos relacionados con la eficiencia, la eficacia y el grado de formalización, asegurando que estos sean claros, medibles y aplicables.

La redacción y documentación de los controles debe realizarse siguiendo los lineamientos establecidos en el numeral 3.2.2 de la presente guía.

Nota: **Ejemplo (continuación):**

Proceso: Gestión de recursos

Objetivo: Gestionar los bienes, obras y servicios administrativos, de mantenimiento y asistencia logística para el cumplimiento de la misión institucional

Alcance: Inicia con la consolidación y depuración del plan de necesidades de bienes, obras y servicios que requieran los procesos institucionales en cada vigencia fiscal y culmina con el suministro de bienes y la prestación de los servicios, acorde con la disponibilidad de recursos

Punto de Riesgo: Ingreso, custodia y salida de bienes muebles de la entidad

Riesgo Fiscal: Posibilidad de efectos dañoso sobre bienes públicos (área de impacto), por pérdida, extravío o hurto de bienes muebles de la entidad (circunstancia inmediata), a causa de la omisión en la aplicación del procedimiento para el ingreso, custodia y salida de bienes e inventario del almacén

Probabilidad Inherente: Media 60%

Impacto Inherente: Catastrófico 100%

Zona de riesgo: Extrema

En la siguiente tabla se muestran los controles propuestos para el riesgo fiscal identificado:

Tipo de control	Descripción	Responsable	Momento de aplicación
Preventivo	El Jefe de Almacén valida y registra diariamente las entradas y salidas en el aplicativo dispuesto para tal fin, el cual alimenta automáticamente el inventario de bienes muebles de la entidad y su responsable	Jefe de Almacén	Entrada del proceso (registro diario)
Detectivo	El Coordinador Administrativo verifica mensualmente la relación de ingresos y salidas de bienes muebles contra los inventarios generados por el sistema. En caso de inconsistencias, solicita al Jefe de Almacén ubicar el bien faltante y realizar el ajuste con los soportes de salida e ingreso correspondientes	Coordinador Administrativo	Durante la ejecución (verificación mensual)
Correctivo	El Director Administrativo verifica la vigencia y actualización de la póliza según los bienes ingresados a la entidad y, en caso de siniestro, adelanta las reclamaciones respectivas ante el asegurador	Director Administrativo	Salida del proceso (ante la materialización del riesgo)

Aplicando la tabla de valoración de controles tenemos:

Control 1: El Jefe de Almacén valida y registra diariamente las entradas y salidas en el aplicativo dispuesto para tal fin, el cual alimenta automáticamente el inventario de bienes muebles de la entidad y su responsable.

Tabla de atributos	*Peso*
Tipo	
Preventivo	**X – 25%**
Detectivo	—
Correctivo	—
Implementación	
Automático	—
Manual	**X – 15%**
Total, Valoración Control 1	**40%**

Control 2: El Coordinador Administrativo verifica mensualmente la relación de ingreso y salida de bienes muebles contra los inventarios generados por el sistema (actualización y ubicación en el inventario). En caso de inconsistencias solicita al Jefe de Almacén ubicar el bien faltante y realizar el ajuste con los soportes de salida e ingreso del almacén.

Tabla de atributos	*Peso*
Tipo	
Preventivo	—
Detectivo	**X – 15%**
Correctivo	—
Implementación	

Automático	—
Manual	**X – 15%**
Total, Valoración Control 2	**30%**

Control 3: El director Administrativo verifica la vigencia y actualización de la póliza de acuerdo con los bienes que ingresan a la entidad y, en caso de presentarse un siniestro, adelanta las reclamaciones respectivas ante el asegurador.

Tabla de atributos	***Peso***
Tipo	
Preventivo	—
Detectivo	—
Correctivo	***X – 10%***
Implementación	
Automático	—
Manual	***X – 15%***
Total, Valoración Control 3	***25%***

Teniendo en cuenta que es a partir de los controles que se dará el movimiento, en la matriz de calor que corresponde a continuación se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles y su respectiva valoración, a fin de determinar el riesgo residual.

El nivel de riesgo residual se determina aplicando de manera acumulativa la efectividad de los controles al riesgo inherente. Esto significa que cada control modifica la probabilidad o el impacto sobre el valor que resulta del control anterior, no sobre el valor inicial.

El ejemplo de la guía muestra el cálculo paso a paso:

- Probabilidad inherente: 60%.
  - Se aplica el control preventivo (40%) → 60% − (60% × 0.40) = 36%.
  - Luego, el control detectivo (30%) → 36% − (36% × 0.30) = 25,2%.
  - Resultado: probabilidad residual = 25,2%.
- Impacto inherente: 100%.
  - Se aplica el control correctivo (25%) → 100% − (100% × 0.25) = 75%.
  - Resultado: impacto residual = 75%.

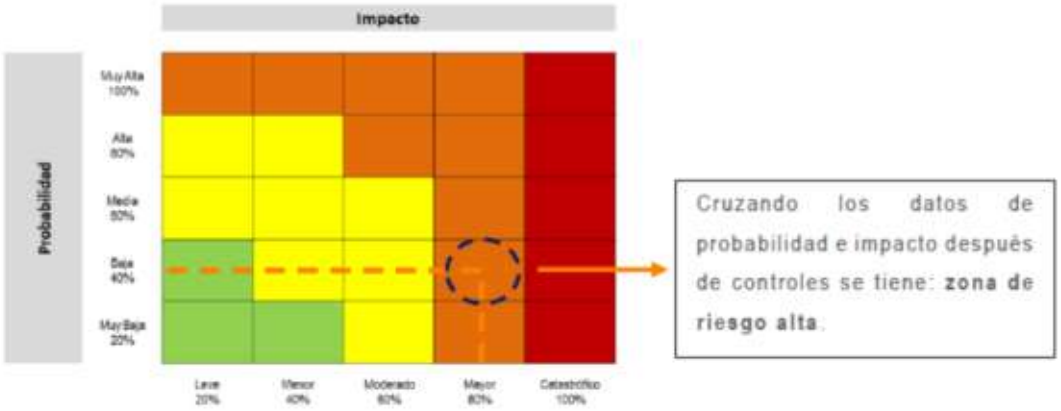
Para mayor claridad a continuación, siguiendo con el ejemplo propuesto, se observan los cálculos requeridos para la aplicación de los tres controles definidos así:

Tabla 25. Ejemplo de aplicación acumulativa de controles para la determinación del riesgo residual

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
Posibilidad de efectos dañoso sobre bienes públicos *(área de impacto)*, **por** pérdida, extravío o hurto de bienes muebles de la entidad *(circunstancia inmediata)*, **a causa de** la omisión de cumplimiento del procedimiento para el ingreso, custodia y salida de bienes e inventario del almacén y el reporte de información a quien gestiona las pólizas cuando haya lugar *(causa raíz)*.	Probabilidad Inherente	60%	Valoración control 1 preventivo	40%	60%* 40% =24% 60% - 24% = **36%**
	Valor probabilidad para aplicar 2o control	**36%**	Valoración control 2 Detectivo	30%	36%* 30% =10.8% 36% - 10,8% = **25,2%**
	Probabilidad Residual	**25,2%**			
	Impacto Inherente	100%	Valoración control correctivo	25%	100%* 25% =25% 100% - 25% = 75%
	Impacto Residual	**75%**			

Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 6. Pág. 81

En la matriz de calor, a continuación, se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles y cálculo final:



La anterior información puede trasladarse a la matriz de riesgo que hace parte de los anexos desarrollados para la presente guía.

VERSIÓN	VIGENTE DESDE	DESCRIPCIÓN
Versión 1	2022	Primera versión de la guía para la administración de riesgos de procesos
Versión 2	2023	Se actualiza la versión 2 incluyendo en la guía los principios para la gestión de riesgos Para mayor claridad se cambió la ilustración 4. Tipología de controles Se ajustó la tabla 7. Tabla de informes de administración de riesgos dando claridad a las fechas de la presentación de los informes/reportes Se actualizó la Ilustración 7. Matriz DOFA Contexto del Proceso, con base en la nueva matriz DOFA Contexto del Proceso Se incluyó el objetivo, las finalidades y actividades del plan de tratamiento cuando el riesgo se encuentre en zona moderada, alta y extrema. Se incluyó el módulo de riesgos de corrupción
Versión 3	2025	1. Se mantiene estructura conceptual para la administración del riesgo. 2. Se incluye capítulo específico sobre riesgo fiscal, que se complementa con el Anexo denominado catalogo indicativo de puntos de riesgo fiscal para facilitar el análisis en el marco del modelo de operación por procesos. 2. Se incluye contenidos relacionados con los riesgos de seguridad de la información, desplegando la totalidad de los pasos metodológicos de acuerdo con lineamientos del Mintic. 3. Se amplían términos y definiciones en concordancia con las actualizaciones en los capítulos.