Política de Administración del Riesgo

Código SG/MIPG	127-PPPVM-02
Vigencia desde	27/05/2026
Versión	5

Proceso

Verificación y mejoramiento continuo

ALCALDÍA MAYOR DE BOGOTÁ D.C.

DEPARTAMENTO ADMINISTRATIVO DE LA DEFENSORÍA DEL ESPACIO PÚBLICO

BOGOTÁ

Tabla de Contenido

1. Introducción

Para el Departamento Administrativo de la Defensoría del Espacio Público – DADEP- es un compromiso desde la gestión y el cumplimiento de resultados, lograr sus objetivos estratégicos, planes, proyectos y procesos institucionales a través de la realización de acciones soportadas en la prevención de los riesgos, implementando controles que promuevan la generación de comportamientos éticos que conlleven a la construcción de una cultura de buen gobierno, que impida la materialización de riesgos de gestión, corrupción y seguridad de la información.

Es así, como el DADEP, de acuerdo con la normatividad vigente y la metodología establecida por el Departamento Administrativo de la Función Pública, diseña la *Política de Administración del Riesgo* como mecanismo para fortalecer el control en los procesos que respondan a los acontecimientos potenciales o aquellos en los que puedan desencadenar situaciones de riesgo de gestión, de corrupción, de seguridad de la información, fiscal y de lavado de activos y financiación del terrorismo, en concordancia con las directrices en materia de gestión pública y el enfoque del Modelo Integrado de Planeación y Gestión- MIPG.

2. Declaración Inicial Política de Administración del Riesgo

El Departamento Administrativo de la Defensoría del Espacio Público se compromete a administrar adecuadamente los riesgos de gestión, de corrupción, de seguridad de la información, fiscales y los de lavado de activos y financiación del terrorismo, asociados a los objetivos estratégicos, planes, proyectos, procesos, trámites y otros procedimientos administrativos (OPAs), considerando la metodología propia para su gestión, determinando oportunamente los controles preventivos y detectivos, para evitar la materialización y la acción correctiva inmediata ante los eventos presentados.

3. Objetivos de la Política de Administración de Riesgos

3.1 Objetivo General de la Política de Administración de Riesgos del DADEP

Administrar los riesgos en el Departamento Administrativo de la Defensoría del Espacio Público - DADEP, haciendo énfasis en el fortalecimiento de los controles internos, con el fin de minimizar la probabilidad de materialización de cualquier tipo de riesgo que afecte el logro de las metas del Departamento.

3.2 Objetivo Específicos

- Generar una visión sistémica de la administración, control y evaluación de los riesgos de la Entidad.
- Proteger los recursos de la entidad, resguardándolos contra la materialización de los riesgos valorados como amenazas de corrupción y/o con un impacto fiscal.
- Introducir y fortalecer dentro de los procesos y procedimientos puntos de control, que permitan evitar, reducir o mitigar, las vulnerabilidades o potenciales amenazas que se puedan presentar.
- Mejorar el aprendizaje organizacional frente a la eficaz identificación y administración de los riesgos.

4. Alcance de la Política de Administración de Riesgos

La política de administración del riesgo es aplicable a todos los servicios, procesos, proyectos, planes y programas de la entidad durante el desarrollo de la gestión planificada y a todas las partes interesadas en el ejercicio de las actividades desarrolladas en el marco de dar cumplimiento a la misionalidad del Departamento Administrativo de la Defensoría del Espacio Público.

5. Roles y Responsabilidades en la Gestión del Riesgos

Con el fin de asegurar que las responsabilidades y autoridades para la gestión del riesgo se asignen, delimiten y comuniquen a los roles pertinentes, la entidad determina la siguiente estructura de gobernanza basada en el modelo de Líneas de Responsabilidad del Manual Operativo del MIPG y los lineamientos vigentes del DAFP:

5.1 Nivel Estratégico

Responsables: Alta Dirección, Comité Institucional de Gestión y Desempeño y Comité Institucional de Coordinación de Control Interno.

Responsabilidades y Funciones:

- Direccionamiento General: Definir, aprobar y supervisar el marco general para la gestión del riesgo, la continuidad del negocio, el control y la política institucional para la administración del riesgo.

- Monitoreo Estratégico: Monitorear y analizar de manera permanente los eventos institucionales, vulnerabilidades, amenazas, escenarios de pérdida de continuidad y riesgos críticos que pongan en peligro el cumplimiento de los objetivos estratégicos, planes, metas y la capacidad institucional para prestar sus servicios.

- Gobernanza: Asegurar la permeabilización de la política en todos los niveles de la organización pública, garantizando el cumplimiento de los planes de la entidad y revisando los cambios del entorno que modifiquen el perfil de riesgo institucional.

- Evaluación de Incidentes: Revisar las acciones ejecutadas ante riesgos materializados, asegurando la toma de medidas oportunas y eficaces para evitar la repetición de los eventos adversos.

5.2 Primera Línea de Responsabilidad

Responsables: Líderes de los planes, programas o proyectos, Líderes de Proceso y otras instancias encargadas de monitorear aspectos estructurales bajo su gestión.

Responsabilidades y Funciones:

- Propiedad del Riesgo: Actuar como los dueños directos del riesgo en la operación. Son responsables de desarrollar, implementar y ejecutar los procesos de control a través de la identificación, análisis, valoración, monitoreo y acciones de mejora en sus respectivas áreas.

- Mitigación Operativa: Implementar rigurosamente los controles identificados y aprobados para mitigar las amenazas asociadas a los planes, programas, proyectos o procesos a su cargo.

- Monitoreo Sectorial: Monitorear de forma específica los aspectos estructurales de los temas bajo su gestión, generando alertas tempranas inmediatas sobre retrasos, incumplimientos u otras situaciones de riesgo detectadas de acuerdo con las materias a su cargo.

- Cultura y Reporte: Divulgar la metodología y las políticas de operación al interior de sus equipos de trabajo, asegurando el reporte oportuno de avances, evidencias y eventos de riesgos materializados ante la Segunda Línea.

5.3 Segunda Línea de Responsabilidad

Esta línea está integrada por las dependencias transversales encargadas de consolidar la metodología, asegurar que los controles estén diseñados apropiadamente y generar alertas agregadas ante el Nivel Estratégico. Se distribuye bajo las siguientes competencias específicas:

A. Oficina Asesora de Planeación

Facilitación Metodológica: Orientar y asesorar a la Primera Línea en la aplicación de la metodología del DAFP, el análisis de causa-raíz y el diseño de controles preventivos o automáticos.

Consolidación: Consolidar de manera integral la gestión del riesgo institucional, construir los mapas de riesgo de la entidad (Gestión y Corrupción) y gestionar su publicación en los canales oficiales de transparencia.

Alertas Estratégicas: Llevar ante el Nivel Estratégico (Alta Dirección y Comités) las alertas consolidadas sobre eventos críticos, desviaciones del perfil de riesgo y cambios en el entorno institucional.

De acuerdo con los lineamientos del Departamento Administrativo de la Función Pública, el Jefe de la Oficina Asesora de Planeación será el Oficial de Cumplimiento para riesgos de gestión, corrupción e integridad (SIGRIP) y lo relacionado con su articulación con el programa de Transparencia Y Ética Pública. Los temas relacionados con seguridad digital, el cumplimiento normativo, tratamiento de datos personales y SARLAFT quedan excluidos de sus competencias, siendo responsabilidad de la OTIC, la Oficina Jurídica e instancias contractuales o inmobiliarias.

B. Subdirección de Gestión Corporativa

Esta instancia asume el monitoreo especializado y la generación de alertas tempranas sobre tres componentes estructurales de la entidad:

- Gestión Contractual: Monitorear de manera permanente la ejecución de la contratación institucional, generando alertas tempranas sobre retrasos, incumplimientos contractuales u otras situaciones de riesgo detectadas en la materia.

- Servicio a la ciudadanía: Monitorear el comportamiento de las Peticiones, Quejas, Reclamos y Denuncias (PQRD), emitiendo alertas oportunas sobre incumplimientos en los términos de respuesta, quejas reiteradas en la prestación del servicio, interposición de acciones de tutela u otras situaciones que afecten la confianza ciudadana.

- Talento Humano: Monitorear de forma integral el ciclo del servidor público (planes de capacitación, bienestar, estímulos e incentivos, convivencia laboral y apropiación del código de integridad), generando alertas sobre riesgos críticos que afecten el clima laboral, incumplimientos normativos o posibles afectaciones al código de integridad institucional.

C. Oficina de Tecnologías de la Información y las Comunicaciones (OTIC)

Esta oficina tiene a cargo las siguientes responsabilidades relacionas con la gestión del riesgo:

- Gestión Tecnológica: Monitorear la ejecución del Plan Estratégico de Tecnologías de la Información (PETI), emitiendo alertas oportunas sobre retrasos, desviaciones presupuestales, incumplimientos técnicos u otras situaciones de riesgo detectadas en materia tecnológica.

- Oficial de Seguridad de la Información: Responsable encargado de evaluar de forma técnica y especializada el cumplimiento de los controles asociados a las políticas de seguridad de la información y privacidad de datos, en el marco del MSPI.

D. Oficina Jurídica

Esta oficina tiene a cargo las siguientes responsabilidades relacionas con la gestión del riesgo:

- Gestión Jurídica y Defensa: Monitorear el estado de la gestión jurídica de la entidad, los procesos judiciales en contra o a favor, y la emisión de conceptos, generando alertas tempranas sobre retrasos, riesgos de pérdida procesal, incumplimientos normativos u otras situaciones de riesgo legal detectadas.

5.4 Tercera Línea de Responsabilidad (Evaluación Independiente)

Responsables: Jefe de la Oficina de Control Interno (o quien haga sus veces).

Responsabilidades y Funciones:

- Aseguramiento Objetivo: Proporcionar una evaluación independiente, objetiva y basada en riesgos sobre la efectividad general del Sistema de Control Interno, auditando de forma ex-post el desempeño y la articulación de la Primera y Segunda Línea de Responsabilidad.

- Suministro de Alertas por Auditoría: Suministrar al Nivel Estratégico alertas tempranas y estructurales sobre retrasos, incumplimientos, fallas en el diseño/ejecución de los controles o situaciones de riesgo crítico detectadas directamente a través de sus seguimientos periódicos y procesos de auditoría interna.

- Independencia Operativa: Salvaguardar su rol evaluador absteniéndose de co-diseñar controles, redactar matrices o participar en la administración activa del riesgo, garantizando la imparcialidad exigida por los entes de control externos y el FURAG.

6. Alineación de la Política con la Plataforma Estratégica de la Entidad

El Departamento Administrativo de la Defensoría del Espacio Público - DADEP fue creado mediante el Acuerdo del Distrito Capital 018 del 31 de julio de 1999, y tiene como principal función la definida en el artículo 3 de la mencionada norma, que establece: “Son funciones de la Defensoría del Espacio Público, sin perjuicio de las atribuciones de otras autoridades, la defensa, inspección, vigilancia, regulación y control del espacio público del Distrito Capital; la administración de los bienes inmuebles, y la conformación del inventario general del patrimonio inmobiliario Distrital”.

Dentro de su misionalidad, el DADEP ha construido una plataforma estratégica, la cual hace parte integral en la definición de los lineamientos de administración de riesgos descritos en esta política.

6.1 Misión:

Contribuir al mejoramiento de la calidad de vida en Bogotá, por medio de una eficaz defensa del espacio público, de una óptima administración del patrimonio inmobiliario de la ciudad y de la construcción de una nueva cultura del espacio público, que garantice su uso y disfrute colectivo y estimule la participación comunitaria.

6.2 Visión:

En 2030, la entidad será líder en la gestión integral del Espacio Público a nivel distrital, contribuyendo a que la ciudadanía disfrute de espacios públicos seguros e inclusivos. Además, seremos referentes en la gestión del patrimonio inmobiliario distrital, la generación de conocimiento urbanístico, la creación de alianzas estratégicas y el fomento de la participación y cultura ciudadana.

6.3 Objetivos Estratégicos:

1. Fomentar la aplicación de los diversos instrumentos de administración del patrimonio inmobiliario distrital y del espacio público, incluyendo proyectos de bienestar de y para la comunidad.

2. Aumentar la oferta cualitativa y cuantitativa de espacio público inclusivo y seguro, con enfoque de género, poblacional, étnico y diferencial.

3. Liderar la gobernanza del espacio público en la ciudad a través de la coordinación interinstitucional e intersectorial de acuerdo con las competencias de las entidades públicas.

4. Fortalecer la capacidad institucional en el marco de un Modelo Integrado de Planeación y Gestión eficiente, que propenda por una gestión pública inteligente, transparente y ágil en la respuesta a los requerimientos de la ciudadanía, promoviendo la participación y el control social.

6.4 Mapa de Procesos:

Ilustración 2. Mapa de Procesos de la Defensoría del Espacio Público

Dentro de los aspectos que la Defensoría del Espacio Público tiene en cuenta para la identificación de los riesgos está la aplicación y adaptación de los lineamientos metodológicos de la Guía del DAFP a las particularidades misionales y competencias jurídicas propias de la entidad. Esto abarca, de manera prioritaria, la identificación de amenazas asociadas a los procesos de incorporación, saneamiento, administración y sostenibilidad del patrimonio inmobiliario distrital, así como la estructuración, adjudicación y seguimiento de los diferentes instrumentos diseñados para garantizar el uso, goce y disfrute del espacio público por parte de la ciudadanía y demás grupos de valor. Este ejercicio técnico se desarrolla bajo el direccionamiento de la Alta Dirección, la cual, a través del Comité Institucional de Gestión y Desempeño y el Comité Institucional de Coordinación de Control Interno, lidera la gestión de riesgos institucional, asegurando la toma de decisiones estratégicas, la cultura de prevención y la protección de los recursos públicos.

7. Compromiso para la Política de Administración de Riesgos

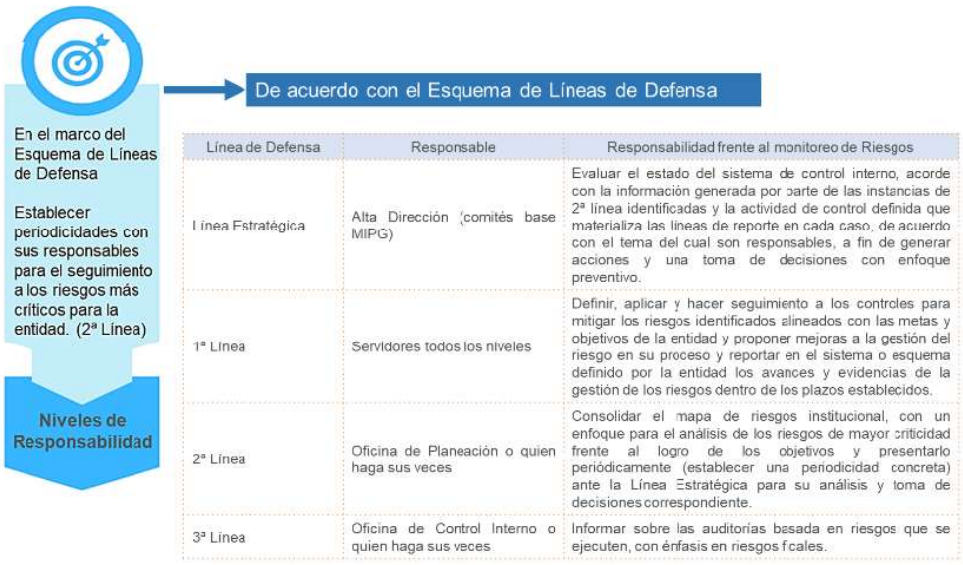
El Departamento Administrativo de la Defensoría del Espacio Público, declara que la Política de Administración de Riesgos representa el compromiso institucional para dar cumplimiento a los lineamientos establecidos en la Guía para la Administración del Riesgo y el diseño de controles en la entidad, en relación con la identificación, análisis, valoración, evaluación, tratamiento y respuesta a los riesgos y escenarios de pérdida de continuidad de negocio que puedan afectar el cumplimiento de los objetivos estratégicos y la adecuada gestión de los procesos, proyectos y planes institucionales, en el marco del Modelo Integrado de Planeación y Gestión- MIPG.

8. Metodología y Normatividad Aplicable

El Departamento Administrativo de la Defensoría del Espacio Público (DADEP) adoptará la metodología establecida por el Departamento Administrativo de la Función Pública (DAFP) en su Guía para la Gestión Integral del Riesgo en Entidades Públicas (Versión 7), marco de referencia bajo el Modelo Integrado de Planeación y Gestión (MIPG). Esta versión evoluciona el enfoque tradicional hacia una gestión basada en la creación de valor, la cultura de la integridad y el esquema de líneas de responsabilidad. Asimismo, en el contexto local, la entidad se acoge a las directrices emanadas por la Secretaría General de la Alcaldía Mayor de Bogotá.

Para una adecuada gobernanza y articulación institucional, el MIPG y el Modelo de Gestión Distrital definen una estructura liderada por la Alta Dirección a través del Comité Institucional de Gestión y Desempeño (CIGD) y el Comité Institucional de Coordinación de Control Interno (CICCI), operando bajo el siguiente esquema de interacción:

Ilustración 4. Gobernanza e Institucionalidad bajo el Modelo de Líneas de Responsabilidad



Línea de Defensa	Responsable	Responsabilidad frente al monitoreo de Riesgos
Línea Estratégica	Alta Dirección (comités base MIPG)	Evaluar el estado del sistema de control interno, acorde con la información generada por parte de las instancias de 2ª línea identificadas y la actividad de control definida que materializa las líneas de reporte en cada caso, de acuerdo con el tema del cual son responsables, a fin de generar acciones y una toma de decisiones con enfoque preventivo.
1ª Línea	Servidores todos los niveles	Definir, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados alineados con las metas y objetivos de la entidad y proponer mejoras a la gestión del riesgo en su proceso y reportar en el sistema o esquema definido por la entidad los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos.
2ª Línea	Oficina de Planeación o quien haga sus veces	Consolidar el mapa de riesgos institucional, con un enfoque para el análisis de los riesgos de mayor criticidad frente al logro de los objetivos y presentarlo periódicamente (establecer una periodicidad concreta) ante la Línea Estratégica para su análisis y toma de decisiones correspondiente.
3ª Línea	Oficina de Control Interno o quien haga sus veces	Informar sobre las auditorías basada en riesgos que se ejecuten, con énfasis en riesgos fiscales.

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas (Versión 7) - DAFP

9. Identificación del riesgo

La identificación de los riesgos le corresponde a la primera línea de defensa a través de los líderes de los procesos con el apoyo de la segunda línea de defensa.

Para ello, es importante definir los cinco (5) tipos de riesgos existentes:

I. Los **Riesgos de Gestión** son aquellos que se asocian al cumplimiento de los procesos y se identifican y/o actualizan cada vigencia por parte de los líderes de los procesos.
II. Los **Riesgos de Corrupción** son aquellos que por acción u omisión afectan negativamente los intereses de la entidad para la obtención de un beneficio particular. A estos riesgos la Oficina de Control Interno les realiza el seguimiento de forma cuatrimestral.
III. Los **Riesgos de Seguridad de la Información** son aquellos que se generan en el entorno digital y que pueden afectar el cumplimiento de objetivos institucionales o de proceso.
IV. Los **Riesgos Fiscales** son aquellos que pueden generar una afectación directa a los recursos públicos.
V. Los **Riesgos de Lavado de Activos y Financiación del Terrorismo** son aquellos que se presentan en eventos susceptibles de este tipo de actividades, utilizando a la Defensoría del Espacio Público como instrumento para generar apariencia de legalidad de recursos ilícitos.

Para realizar una correcta identificación del riesgo se debe establecer el contexto tanto interno como externo de la entidad y la descripción y clasificación del riesgo.

9.1 Establecimiento del contexto de la entidad

Una vez determinados estos lineamientos básicos, es preciso analizar el contexto general de la entidad para establecer su complejidad, procesos y planeación institucional, entre otros aspectos, lo que permite conocer y entender la entidad y su entorno, determinando una especificidad necesaria en el análisis de riesgos y la aplicación de la metodología en general.

Para la identificación de los riesgos que estén o no bajo el control de la entidad, se debe tener en cuenta el contexto estratégico en el que opera la misma, la caracterización de cada proceso que contempla su objetivo y alcance y, también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos; por lo tanto, los factores internos y externos para la administración del riesgo en la Defensoría del Espacio Público son los siguientes:

9.2 Factores del Contexto Externo que pueden afectar el funcionamiento del Departamento Administrativo de la Defensoría del Espacio Público

Políticos: Cambios de gobierno, legislación, políticas públicas y regulación (Cambios en la administración central y territorial que genera cambios en los planes de desarrollo).

Económicos y financieros: disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia; restricciones de orden económico que pueden afectar el funcionamiento de la entidad o la ejecución de los proyectos; cambios en la asignación presupuestal de la entidad por cambio de prioridades de la administración.

Sociales y culturales: Demografía, responsabilidad social y orden público; mayor demanda de espacio público por incremento de migración de población hacia Bogotá y desplazamiento de esta a la periferia de la ciudad y sus municipios circunvecinos; requerimientos de las partes interesadas externas (vecinos, comerciantes, alcalde, concejales).

Tecnológicos: Avances en tecnología, acceso a sistemas de información externos, gobierno en línea.

Ambientales: Emisiones y residuos, catástrofes naturales y desarrollo sostenible; cambio de las políticas que propendan por disminuir la afectación ambiental a través de procesos de mitigación de impacto ambiental.

Legales y reglamentarios: Normatividad externa (leyes, decretos, ordenanzas y acuerdos) en diferentes ámbitos (laboral, contractual, administración del espacio público, sectorial, entre otros) que afecte la gestión de la entidad.

9.3 Factores del Contexto Interno que pueden afectar el funcionamiento del Departamento Administrativo de la Defensoría del Espacio Público

Financieros: presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.

Personal: competencia del personal, disponibilidad, seguridad y salud ocupacional.

Procesos: capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.

Tecnología: integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información.

Estratégicos: direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo.

Comunicación Interna: canales utilizados y su efectividad, flujo de la información adecuado.

9.4 Factores del Contexto del Proceso que pueden afectar el funcionamiento del Departamento Administrativo de la Defensoría del Espacio Público

Diseño del proceso: claridad en la descripción del alcance y objetivo del proceso.

Interacciones con otros procesos: relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.

Transversalidad: procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.

Procedimientos asociados: pertinencia en los procedimientos que desarrollan los procesos.

Responsables del proceso: grado de autoridad y responsabilidad de los funcionarios frente al proceso.

Comunicación entre los procesos: efectividad en los flujos de información determinados en la interacción de los procesos.

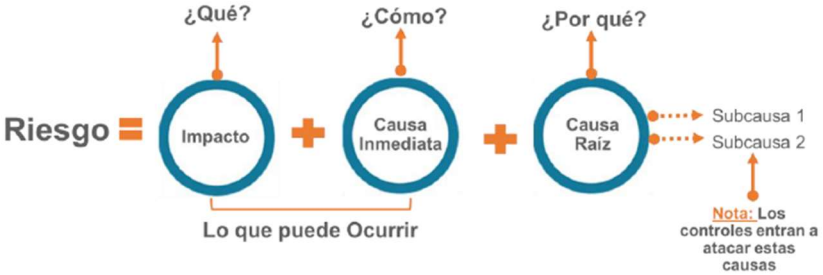
Activos de seguridad de la información del proceso: información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso.

9.5 Descripción del riesgo

La descripción del riesgo debe ser lo suficientemente detallada de tal forma que sea entendible tanto para el líder y los servidores que desarrollan el proceso, como para personas ajenas al mismo.

En tal sentido y continuando con lo recomendado en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades públicas del Departamento Administrativo de la Función Pública, la estructura de la redacción de los riesgos inicia con la frase POSIBILIDAD DE y se desarrolla de la siguiente manera:

Ilustración 5. Estructura de la redacción del riesgo



Fuente: Guía para la Administración del Riesgo

9.6 Clasificación del riesgo

La clasificación del riesgo permite agrupar los riesgos identificados en los diferentes procesos de la Defensoría del Espacio Público y para ello se tendrán las siguientes categorías:

Ilustración 6. Categorías de los riesgos

Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
Fallas tecnológicas	Errores en *hardware*, *software*, telecomunicaciones, interrupción de servicios básicos.
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

Fuente: Guía para la Administración del Riesgo DAFP

Para una mayor claridad y teniendo en cuenta los factores de riesgo que la Defensoría del Espacio Público identifica, se puede establecer una interrelación entre éstos y las categorías de los riesgos, así:

Ilustración 7. Relación entre factores y clasificación del riesgo

Fuente: Guía para la Administración del Riesgo

10. Valoración del riesgo

La valoración del riesgo busca establecer la probabilidad de ocurrencia y el nivel de impacto del riesgo con el fin de determinar la zona del riesgo inicial (riesgo inherente), para lo cual es necesario realizar:

- Análisis de riesgos
- Evaluación de riesgos
- Monitoreo y revisión
- Seguimiento

10.1 Análisis de riesgos

Para iniciar con la etapa de análisis es necesario determinar la posibilidad de ocurrencia de un riesgo, por lo cual se adoptan los siguientes criterios para clasificar la probabilidad del riesgo en la Defensoría del Espacio Público:

Ilustración 8. Criterios para definir el nivel de probabilidad de los riesgos con excepción de los de corrupción

DESCRIPCIÓN	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%
Ejemplo: La actividad se realiza 120 veces al año, la probabilidad de ocurrencia del riesgo es media.		

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades Públicas del DAFP

Así mismo, la Defensoría determina los siguientes criterios para definir el nivel de impacto de los riesgos, así:

Ilustración 9. Criterios para definir el nivel de impacto de los riesgos, con excepción de los de corrupción

DESCRIPCIÓN	Afectación Económica o Presupuestal	Pérdida Reputacional
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de alguna área de la organización

DESCRIPCIÓN	Afectación Económica o Presupuestal	Pérdida Reputacional
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta directiva y accionistas y/o de proveedores
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitarios sostenible a nivel país
Ejemplo: La afectación económica se calcula en 500 SMLMV, el impacto del riesgo es mayor.		

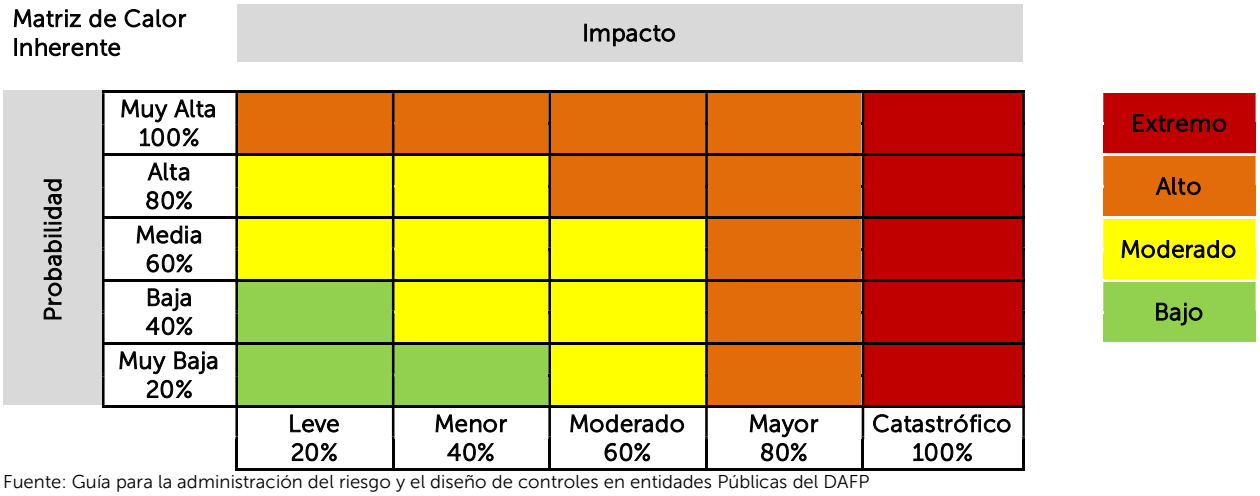
Fuente: Guía para la administración del riesgo y el diseño de controles en entidades Públicas del DAFP

10.2 Evaluación de los riesgos

La evaluación se realiza una vez se ha realizado el análisis de la probabilidad y del impacto del riesgo, con el fin de determinar la zona de riesgo inicial (riesgo inherente).

Para iniciar la evaluación se hace necesario determinar los niveles de severidad a través de la ubicación del riesgo en el Mapa de Calor de acuerdo con el resultado que se genere a partir de la combinación entre la probabilidad y el impacto del riesgo.

Ilustración 10 . Mapa de Calor



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades Públicas del DAFP

Posterior a la identificación de los niveles de severidad, se debe estructurar el control o los controles, entendidos estos como las medidas que permiten reducir o mitigar el riesgo. Es

preciso aclarar que a cada riesgo se le deben identificar los controles y los responsables de implementarlos y monitorearlos son los líderes de los procesos.

La estructura para la descripción del control será la siguiente:

Responsable de ejecutar el control	+	Acción	+	Complemento
¿Quién?		¿Qué?		¿Cómo?

Existen tres (3) tipos de controles, a saber:

I. Controles Preventivos: son aquellos que atacan las causas y con ello, la probabilidad de ocurrencia del riesgo.
II. Controles Detectivos: son aquellos que se ejecutan durante la ejecución del proceso, es decir, que detectan los riesgos.
III. Controles Correctivos: son aquellos que atacan el impacto frente a la materialización del riesgo.

10.2.1. Nivel de Riesgo

Una vez se mide la efectividad de la aplicación del control o los controles al riesgo inicial o inherente, se hace necesario identificar el riesgo residual. Para ello, se debe identificar la probabilidad residual de la siguiente manera:

Probabilidad inherente (%) * Valoración del Control Preventivo (%) = X
Probabilidad inherente (%) – X = Valor de la probabilidad para aplicar el 2° control (%)
Valor de la probabilidad para aplicar el 2° control (%) * Valoración del Control Detectivo (%) = Y
Valor de la probabilidad para aplicar el 2° control (%) – Y = **Probabilidad Residual (%)**

Por su parte, el valor del **Impacto Residual** es el mismo del valor del Impacto Inicial o Inherente, toda vez que no se tienen controles para mitigar el impacto.

Una vez se tienen identificadas tanto la probabilidad residual como el impacto residual, éstas se combinan en el mapa de calor de la Defensoría del Espacio Público (ilustración 10) y allí se determina el movimiento en el mapa evidenciando la efectividad de los controles aplicados.

11. Lineamientos para Riesgos de Seguridad de la Información

Se debe tener en cuenta que la política de seguridad de la información se vincula al modelo de seguridad y privacidad de la información (MSPI), el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital: seguridad de la información, arquitectura, servicios ciudadanos digitales.

Los riesgos de seguridad de la información se basan en la afectación de tres pilares en un activo o tipos de activos de información dentro del proceso: "Integridad, confidencialidad o disponibilidad". Se identificarán riesgos de seguridad de la información a los activos o tipos de activos de información que se encuentren clasificados como críticos en el proceso, de acuerdo con la documentación de activos de información de la Entidad.

Existen tres tipos de riesgos asociados a seguridad de la información, entre los que se incluyen: pérdida de confidencialidad, pérdida de la integridad y pérdida de la disponibilidad de los activos de información.

Las amenazas y vulnerabilidades comunes a todas las entidades del sector público pueden ser consultadas en el documento "Anexo 4 Modelo Nacional de Gestión de riesgos de Seguridad de la Información en Entidades Públicas del Ministerio de Tecnologías de la Información y Comunicaciones (MinTIC).

11.1 Identificación de los activos de seguridad de la información

Como primer paso para la identificación de riesgos de seguridad de la información es necesario identificar los activos de información del proceso.

Ilustración 11. Identificación activos de información.

¿Qué son los activos?	¿Por qué identificar los activos?
Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como: -Aplicaciones de la organización	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).
¿Qué son los activos?	**¿Por qué identificar los activos?**
-Servicios web -Redes -Información física o digital -Tecnologías de información TI -Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital	La entidad puede saber **qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano**, aumentando así su confianza en el uso del entorno digital.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas DAFP

Para la identificación de los activos de información debe cumplirse con los siguientes pasos:

Ilustración 12. Pasos identificación activos de información

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

Para realizar la identificación de activos 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" que hace parte de la Guía para la Administración de Riesgos y Controles, Versión 5 del año 2020.

Ejemplo identificación activos del proceso:

Ilustración 13. 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 completitud o integridad	Criticidad respecto a su disponibilidad	Nivel de criticidad
Gestión financiera	Base de datos de nómina	Base de datos con información de nómina de la entidad	Jefe de oficina financiera	Información	Información reservada	No contiene datos personales	ALTA	ALTA	ALTA	ALTA
Gestión financiera	Aplicativo de nómina	Servidor web que contiene el *front office* de la entidad	Jefe de oficina financiera	Software	N/A	N/A	BAJA	MEDIA	BAJA	MEDIA
Gestión financiera	Cuentas de cobro	Formatos de cobro diligenciados	Jefe de oficina financiera	Información	Información pública	No contiene datos personales	BAJA	BAJA	BAJA	BAJA

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas DAFP

11.2 Identificación de los activos de seguridad de la información

Se podrán identificar tres (3) tipos de riesgos inherentes de seguridad de la información:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para cada riesgo se deben asociar el grupo de activos o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. Para este efecto, es necesario consultar el Anexo 4 Modelo nacional de gestión

de riesgos de seguridad de la información para entidades públicas que hace parte de la Guía para la Administración de Riesgos y Controles Versión 6 del año 2022.

Para la construcción de los riesgos de seguridad de la información, es necesario contar con la siguiente información:

Ilustración 14. Información requerida para la construcción de los riesgos de seguridad de la información

RIESGO	ACTIVO	DESCRIPCIÓN DEL RIESGO	AMENAZA	TIPO	CAUSAS/ VULNERA-BILIDADES	CONSECUENCIAS
Base de datos de nómina	Pérdida de la integridad	La falta de políticas de seguridad digital, ausencia de políti-cas 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	Posibles consecuencias que pueda enfrentar la entidad o el proceso a causa de la materialización del riesgo(legales, económicas, sociales, reputacionales, confianza en el ciudadano). Ej.: posible retraso en el pago de nómina.
					Ausencia de políticas de control de acceso	
					Contraseñas sin protección	
					Autenticación débil	

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas DAFP

11.3 Infraestructura Crítica Cibernética

Los riesgos de seguridad de la información deben tener en cuenta los criterios de criticidad en las variables definidas en la Guía para la Identificación de Infraestructura Crítica Cibernética - ICC- de Colombia, para la valoración del impacto de afectación de los servicios esenciales de acuerdo con su nivel de criticidad:

- **El impacto social:** Valorado en función de la afectación de la población (incluyendo pérdida de vidas humanas), el sufrimiento físico y la alteración de la vida cotidiana (se estima como el 0,5% de la población total colombiana).
- **El impacto económico:** Valorado en función de la magnitud de las pérdidas económicas en relación con el Producto Interno Bruto de Colombia – PIB – (Se estima como el PIB diario o el 0,123% del PIB anual).
- **Impacto medioambiental:** Valorado en función de los años que tarda la recuperación del medio ambiente (se estima como 3 años).

Es por lo anterior que también se podrá tener en cuenta la siguiente tabla de valoración de impacto para los Riesgos de Seguridad de la Información:

Ilustración 15. Valoración de impacto de Riesgos Seguridad de la Información

Nivel	Valor del Impacto	Impacto (Consecuencias) Cuantitativo	Impacto (Consecuencias) Cualitativo
CATASTRÓFICO	5	Afectación en un valor ≥ 50% de la población. Afectación en un valor ≥ 50% del presupuesto anual de la entidad Afectación muy grave del medio ambiente que requiere ≥ 3 años de recuperación.	Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros. Interrupción de las operaciones de la Entidad por más de cinco 5 días
MAYOR	4	Afectación en un valor ≥ 20% e inferior al 50% de la población. Afectación en un valor ≥ 20% e inferior al 50% del presupuesto de la entidad. Afectación importante del medio ambiente que requiere de 1 a 3 años de recuperación.	Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros. Interrupción de las operaciones de la Entidad entre 2 y 4 días
MODERADO	3	Afectación en un valor ≥ 10% y menor al 20% de la población. Afectación en un valor ≥ 10% y menor al 20% del presupuesto de seguridad de la información en la entidad. Afectación leve del medio ambiente requiere de 3,1 a 1 año de recuperación.	Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros. Interrupción de las operaciones de la Entidad por un (1) día.
MENOR	2	Afectación en un valor ≥ 1% y menor al 10%de la población. Afectación en un valor ≥ 1% y menor al 10%del presupuesto de seguridad de la información en la entidad. Afectación leve del medio ambiente requiere de 1 a 3 meses de recuperación.	Afectación leve de la integridad. Afectación leve de la disponibilidad. Afectación leve de la confidencialidad Interrupción de las operaciones de la Entidad hasta por 8 horas (1 jornada laboral)
INSIGNIFICANTE	1	Afectación en un valor menor al 1% de la población. Afectación en un valor menor al 1% del presupuesto de seguridad de la información en la entidad. No hay afectación medioambiental.	Sin afectación de la integridad. Sin afectación de la disponibilidad. Sin afectación de la confidencialidad No hay interrupción de las operaciones de la entidad

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades Públicas del DAFP

Para la valoración del riesgo es importante tener en cuenta:

Ilustración 16. Variables a tener en cuenta para la valoración de los riesgos de seguridad de la información

Las variables confidencialidad, integridad y disponibilidad se definen de acuerdo con el modelo de seguridad y privacidad de la información de la estrategia de Gobierno Digital (GD) del Ministerio de Tecnologías de la Información y las Comunicaciones.
La variable población se define teniendo en cuenta el establecimiento del contexto externo de la entidad, es decir, que la consideración de población va a estar asociada a las personas a las cuales se les prestan servicios o trámites en el entorno digital y que de una u otra forma pueden verse afectadas por la materialización de algún riesgo en los activos identificados. Los porcentajes en las escalas pueden variar, según la entidad y su contexto.
La variable presupuesto es la consideración de presupuesto afectado por la entidad debido a la materialización del riesgo, contempla sanciones económicas o impactos directos en la ejecución presupuestal.
La variable ambiental estará también alineada con la afectación del medio ambiente por la materialización de un riesgo de seguridad digital. Esta variable puede no ser utilizada en la mayoría de los casos, pero debe tenerse en cuenta, ya que en alguna eventualidad puede existir afectación ambiental.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas DAFP

11.4 Controles asociados a la seguridad de la información

La entidad podrá mitigar/tratar los riesgos de seguridad de la información empleando como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, estos controles se encuentran en el anexo 4. "Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas", y deben tenerse en cuenta para el análisis de riesgos. Acorde con el control seleccionado, será necesario considerar las características de diseño y ejecución definidas para su valoración.

Ilustración 17. características de diseño y ejecución de los riesgos de seguridad de la información

Procedimientos operacionales y responsabilidades	Objetivo: asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información
Procedimientos de operación documentados	Control: los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
Gestión de cambios	Control: se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
Gestión de capacidad	Control: para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, llevar a cabo los ajustes y las proyecciones de los requisitos sobre la capacidad futura.
Separación de los ambientes de desarrollo, pruebas y operación	Control: se deberían separar los ambientes de desarrollo, prueba y operación para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
Protección contra códigos maliciosos	Objetivo: asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
Controles contra códigos maliciosos	Control: se deberían implementar controles de detección, prevención y recuperación, combinados con la toma de conciencia apropiada por parte de los usuarios para protegerse contra códigos maliciosos.
Copias de respaldo	Objetivo: proteger la información contra la perdida de datos.
Respaldo de información	Control: se deberían hacer copias de respaldo de la información, del *software* y de las imágenes de los sistemas, ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas DAFP

12. Lineamientos para Riesgos de Corrupción

El riesgo de corrupción es la posibilidad de que, por acción u omisión, se utilice la gestión pública para un beneficio privado.

12.1 Descripción del riesgo:

Los componentes que deben concurrir para la descripción de los riesgos de corrupción de la Defensoría del Espacio Público son:

Acción u Omisión + Uso del poder + Desviación de la gestión de lo público + El beneficio privado

Ejemplo:

Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato sin el cumplimiento de requisitos legales

12.2 Análisis del riesgo:

Para los riesgos de corrupción, la probabilidad de ocurrencia del riesgo se expresa en términos de frecuencia, la cual implica analizar el número de eventos en un periodo determinado, es decir, hechos que se han materializado o se cuenta con datos de situaciones asociadas ocurridas en vigencias anteriores. Es por ello por lo que la valoración de probabilidad para los riesgos de corrupción se establece en la siguiente ilustración:

Ilustración 18. Valoración de probabilidad de Riesgos de Corrupción

PROBABILIDAD			
NIVEL	DESCRIPCIÓN	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 podría 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.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades Públicas del DAFP.

Así mismo, en lo que se refiere a la medición del impacto de los riesgos de corrupción, ésta se determina a partir de unos criterios que califican las consecuencias identificadas en la descripción del riesgo, así:

Ilustración 19. Medición de impacto de riesgos de Corrupción

IMPACTO CORRUPCIÓN			
NOMBRE DEL RIESGO DE CORRUPCION			
Posibilidad de alterar o manipular información			
No.	SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...	RESPUESTA	
		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 o servicios o los recursos públicos?		

IMPACTO CORRUPCIÓN			
NOMBRE DEL RIESGO DE CORRUPCION			
Posibilidad de alterar o manipular información			
No.	SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...	RESPUESTA	
		SI	NO
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?		
TOTAL RESPUESTAS AFIRMATIVAS		0	

Responder afirmativamente de 1 a 5 pregunta(s) genera un impacto **Moderado - 3**.
Responder afirmativamente de 6 a 11 preguntas genera un impacto **Mayor - 4**.
Responder afirmativamente de 12 a 19 preguntas genera un impacto **Catastrófico- 5**.
MODERADO Genera medianas consecuencias sobre la entidad
MAYOR Genera altas consecuencias sobre la entidad
CATASTRÓFICO Genera consecuencias desastrosas para la entidad
Fuente: Guía para la administración del riesgo y el diseño de controles en entidades Públicas del DAFP

Estas calificaciones serán plasmadas en las herramientas denominadas mapas de calor para corrupción, donde se graficarán las probabilidades de ocurrencia de los riesgos analizados, tanto para los riesgos inherentes, como los riesgos residuales después de la implementación de controles.

Ilustración 20. Mapa de Calor para Riesgos de Corrupción

PROBABILIDAD	IMPACTO				
	Insignificante(1)	Menor(2)	Moderado(3)	Mayor(4)	Catastrófico(5)
Casi Seguro (5)	Calificación 5 Zona de riesgo alta	Calificación 10 Zona de riesgo alta	Calificación 15 Zona de riesgo extrema	Calificación 20 Zona de riesgo extrema	Calificación 25 Zona de riesgo extrema
Probable (4)	Calificación 4 Zona de riesgo moderada	Calificación 8 Zona de riesgo alta	Calificación 12 Zona de riesgo alta	Calificación 16 Zona de riesgo extrema	Calificación 20 Zona de riesgo extrema
Posible (3)	Calificación 3 Zona de riesgo baja	Calificación 6 Zona de riesgo moderada	Calificación 9 Zona de riesgo alta	Calificación 12 Zona de riesgo extrema	Calificación 15 Zona de riesgo extrema
Improbable (2)	Calificación 2 Zona de riesgo baja	Calificación 4 Zona de riesgo baja	Calificación 6 Zona de riesgo moderada	Calificación 8 Zona de riesgo alta	Calificación 10 Zona de riesgo extrema
Rara vez (1)	Calificación1 Zona de riesgo baja	Calificación 2 Zona de riesgo baja	Calificación 3 Zona de riesgo moderada	Calificación 4 Zona de riesgo alta	Calificación 5 Zona de riesgo alta

Nivel de Severidad	Bajo	Moderado	Alto	Extremo

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades Públicas del DAFP

13. Lineamientos para los Riesgos Fiscales

13.1 Identificación de riesgos fiscales

Para la identificación de los riesgos fiscales es necesario iniciar con la identificación de los **puntos de riesgo fiscal**, es decir, las actividades que representen gestión fiscal en la Defensoría y aquellas que han generado advertencias, hallazgos fiscales y/o fallos de responsabilidad fiscal, además de identificar las **circunstancias inmediatas** que corresponden a las situaciones o actividades bajo las cuales se presenta el riesgo, pero que no constituyen su causa raíz.

Identificación de áreas de impacto: el área de impacto es una consecuencia económica sobre el patrimonio público en caso de materializarse el riesgo.

Identificación de la causa raíz: es cualquier evento potencia (acción u omisión) que de presentarse generaría una consecuencia económica sobre el patrimonio público. Ejemplo: La omisión de un pago oportuno.

13.2 Descripción del riesgo fiscal

Para redactar un riesgo fiscal se tendrá en cuenta:

- Inicia con "Posibilidad de", ya que es un evento potencial.
- Continúa con el impacto, es decir, el efecto dañoso que corresponde al qué.
- Sigue con la circunstancia inmediata, la cual corresponde al cómo.
- Finaliza con la causa raíz que equivale al por qué.

Ejemplo:

Ilustración 21. Ejemplo de descripción de un riesgo fiscal

¿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

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades Públicas del DAFP

14. Niveles de aceptación al riesgo

La gestión del riesgo en la Defensoría del Espacio Publicó se seguirá gestionando, mediante la aplicación de la línea estratégica y las tres líneas de defensa establecidas en el Modelo

Integrado de Planeación y Gestión MIPG, durante las etapas de desarrollo de la gestión institucional y se establecen los niveles de aceptación del riesgo así:

14.1 Riesgos a Controlar – Administrar

Se establece que la totalidad de riesgos identificados en el mapa de riesgos institucional y por procesos estarán sujetos al seguimiento, monitoreo, control y ajuste mediante la aplicación de la metodología establecida por el Departamento Administrativo de la Función Pública.

Para los riesgos de Gestión, Fiscales y de Seguridad de la Información se establece el siguiente nivel de aceptación:

- Zona de riesgo **BAJO**: Se asumirá el riesgo y se administra por medio de las actividades propias del proyecto o proceso asociado.

- Zona de riesgo **MODERADO**: Se establecen acciones de control preventivas que permitan reducir la probabilidad de ocurrencia del riesgo.

- Zona de riesgo **ALTO**: Se establecen acciones de control preventivas que permitan mitigar la materialización del riesgo.

- Zona de riesgo **EXTREMO**: se establecen acciones de Control Preventivas y correctivas que permitan mitigar la materialización del riesgo.

El Departamento Administrativo de la Defensoría del Espacio Público-DADEP establece las acciones a seguir por el líder de proceso ante la materialización del riesgo de corrupción, así:

- Informar al Proceso de Direccionamiento Estratégico sobre el hecho encontrado.
- Realizar la denuncia ante la instancia de control correspondiente (cuando se requiera).
- Identificar las acciones correctivas necesarias y documentarlas en el Plan de mejoramiento.
- Actualizar el mapa de riesgos.
- Ante la materialización del riesgo de gestión en zona alta, extrema y moderada se procede de manera inmediata a aplicar el plan de contingencia que permita la continuidad del servicio o el restablecimiento del mismo (si es el caso) y documentarlo en el Plan de mejoramiento.

14.2 Apetito del Riesgo

El apetito al riesgo es el nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, su marco legal y las disposiciones de la alta dirección. De acuerdo con lo anterior, en el Departamento Administrativo de la Defensoría del Espacio Público el apetito del riesgo es el riesgo residual (luego de aplicar controles) que se ubica en la zona baja y por consiguiente no requiere generar acciones adicionales.

Este apetito del riesgo debe contemplarse en los monitoreos periódicos, por lo cual se tiene que revisar, al igual que los demás riesgos, la ejecución de los controles, esto con el fin de que se evalúe constantemente si el riesgo permanece en zona baja o si por el contrario se requiere actualizar la valoración del riesgo que lo ubique en zona moderada, alta o extrema, modificando de esta manera el apetito inicial del riesgo. Para el caso de los riesgos de corrupción, es de anotar que por su naturaleza estos no se ubican en zona de riesgo baja.

14.3 Tolerancia al 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. En la Defensoría del Espacio Público, teniendo en cuenta que el apetito del riesgo es para riesgos residuales que se ubiquen en zona baja y que la aceptación de riesgos debe aprobarse por la Alta Dirección, el nivel de tolerancia al riesgo es de cero, es decir, la ejecución de controles y planes de acción debe ser completa y no parcial. Así mismo, complementario al nivel cero de tolerancia, el DADEP mediante la identificación de controles, dispuso el campo "Actividades para gestionar en caso de materialización de riesgo" allí se determinaron las acciones a realizar en caso de que falle la ejecución de controles, por lo que un evento de materialización de riesgo tendrá que reportarse y solucionarse.

14.4 Plan de Manejo de Riesgos

Los planes de manejo son el conjunto de actividades (acciones) encaminadas a realizar el tratamiento del riesgo, en ellos se identifica los responsables, las fechas de cumplimiento y los indicadores para medir la eficacia de las acciones implementadas.

Adicionalmente, si al valorar los riesgos estos resultan en zona de riesgo "Extrema", se puede formular opcionalmente un Plan de Contingencia cuyo contenido proyecta aquellas acciones inmediatas a ejecutar en caso de la materialización del riesgo. Esto evita que se presente inconvenientes en el cumplimiento de los objetivos de la Entidad.

Los responsables de las tareas deberán realizar sus reportes cada cuatro meses respecto al avance de estas, de manera tal que la Oficina de Control Interno pueda realizar seguimiento a la efectividad de las medidas para mitigar el riesgo.

15. Escenarios de pérdida de continuidad

Los escenarios de riesgo corresponden a descripciones de situaciones que agrupan la ocurrencia de uno o más riesgos que generan la pérdida de continuidad en las actividades institucionales. La entidad adopta el siguiente conjunto de escenarios de riesgo estandarizados para el diseño de la estrategia de continuidad de negocio:

Ilustración 22. Escenarios de pérdida de continuidad

Escenario	Descripción
Emergencia Social	Imposibilidad de uso de las instalaciones debido a revueltas sociales, asonadas o pérdida del orden público que hace imposible la prestación del servicio o generación del producto.
Desastre Natural y Colapso de Infraestructura Física	Imposibilidad de acceso o abandono súbito de las instalaciones debido a un caso fortuito, fenómeno natural o fuerza mayor.
Desastre Tecnológico	Pérdida total de la capacidad tecnológica o delos procesos institucionales para prestar los servicios o generar los productos.
Crisis Financiera	Inexistencia de los bienes y servicios necesarios para el normal funcionamiento de la entidad que impacta la disponibilidad de recursos financieros, humanos, físicos y tecnológicos
Endemia y Pandemia	Crisis sanitaria que impide el funcionamiento de los procesos institucionales, incluye pandemias y epidemias declaradas por los organismos de salud del Estado.

Cuando se presentan eventos que materializan uno o más de los escenarios de continuidad del negocio la Entidad evaluará las características de la emergencia para autorizar la activación del plan de continuidad, designar recursos y autorizar cualquier comunicación oficial hacia todos los grupos de valor, una vez declarada oficialmente la emergencia, se aplican las acciones de respuesta definidas en el plan de continuidad de negocio para dar respuesta a la misma.

16. Acciones ante los riesgos materializados

A continuación, se establecen las acciones de respuesta a adelantar para cuando se materializan riesgos identificados en la matriz de riesgos. Según el tipo de riesgo, el líder de proceso debe:

Riesgos Fiscales y de Corrupción	Riesgos de Gestión por proceso	Riesgos de Seguridad de la información
1. En articulación con el Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP), la materialización de un riesgo de corrupción (soborno, fraude, inadecuada gestión del conflicto de intereses o LA/FT/FP) exige un tratamiento de máxima criticidad, orientado a proteger el patrimonio público y la confianza institucional: 2. El evento debe ser informado inmediatamente al Oficial de Cumplimiento (Jefe de la Oficina Asesora de Planeación), garantizando absoluta reserva de la información y la activación de los mecanismos de protección a denunciantes. 3. Si el hecho reviste características de delito, detrimento patrimonial o falta disciplinaria, la Oficina Asesora Jurídica y la Oficina de Control Interno Disciplinario iniciarán de forma perentoria los traslados procesales a los entes de control competentes (Fiscalía, Contraloría, Personería). 4. Evaluar rigurosamente si fallaron los mecanismos de conocimiento de la contraparte, con especial énfasis en los contratos de aprovechamiento económico del espacio público (CAMEP), la administración de zonas de cesión y los convenios con terceros. 5. Informar al proceso de Direccionamiento Estratégico y al Comité Institucional de Gestión y Desempeño sobre el riesgo materializado y los ajustes realizados a la definición del riesgo y los controles que fallaron. 6. Ajustar en un plazo no mayor a 30 días, el Mapa de Riesgos de Corrupción, redefiniendo las políticas de operación, fortaleciendo la segregación de funciones y eliminando los focos de discrecionalidad en los trámites que facilitaron la materialización.	1. Documentar el evento detallando la fecha, el proceso afectado, la desviación generada y la magnitud real del impacto operativo. 2. Evaluar si el evento ocurrió por la manifestación de una causa ya documentada, la aparición de un factor de riesgo externo/interno no previsto, o la inoperancia del control existente (falla de diseño o de ejecución). 3. El evento debe ser informado inmediatamente al Oficial de Cumplimiento (Jefe de la Oficina Asesora de Planeación) 4. Establecer acciones correctivas al interior de cada proceso, a cargo del líder respectivo y verificar la calificación y ubicación del riesgo para su inclusión en el mapa de riesgos. 5. Se requiere realizar el ajuste obligatorio de la matriz, ya que es necesario elevar el nivel de probabilidad, lo cual afecta directamente la valoración del riesgo. Asimismo, se debe ajustar el nivel de impacto si el daño real superó la estimación inicial. 6. Sustituir o fortalecer los controles que fallaron. Formular planes de acción orientados a transitar de controles netamente detectivos o manuales hacia controles preventivos y automáticos. 7. Informar al proceso de Direccionamiento Estratégico y al Comité Institucional de Gestión y Desempeño sobre el riesgo materializado y los ajustes realizados a la definición del riesgo y los controles que fallaron. 8. El riesgo materializado, no podrá ser eliminado de la matriz, al menos hasta que las causas que dieron origen a la materialización sean mitigadas.	1. El área de Tecnologías de la Información (TI) o quien haga sus veces aplicará los protocolos de respuesta técnica para aislar los activos de información afectados y mitigar la propagación de la amenaza (ej. suspensión de accesos, desconexión de redes). 2. Determinar de forma inmediata la dimensión del impacto sobre la Confidencialidad (accesos no autorizados a bases de datos), la Integridad (alteración no autorizada de inventarios inmobiliarios) o la Disponibilidad (caída de sistemas misionales críticos). 3. Contrastar la brecha que originó el incidente contra el Inventario de Activos de Información. Identificar si la falla fue de origen tecnológico, humano (ingeniería social) o físico. 4. Replantear la matriz de seguridad. Si el impacto superó la capacidad de los controles técnicos internos, la Alta Dirección deberá definir nuevas estrategias de tratamiento, tales como la transferencia del riesgo (ej. adquisición de ciberpólizas) o el rediseño del Plan de Continuidad de Negocio (BCP) y Recuperación ante Desastres (DRP). 5. al Oficial de Cumplimiento (Jefe de la Oficina Asesora de Planeación) sobre el riesgo materializado y los ajustes realizados a la definición del riesgo y los controles que fallaron. 6. En caso de que el incidente comprometa el tratamiento de datos personales de ciudadanos o funcionarios, se deberá cumplir con el reporte obligatorio de incidentes ante la Superintendencia de Industria y Comercio (SIC) en los tiempos establecidos por la ley.

17. Herramientas para la Gestión del Riesgo

Las diferentes etapas con sus entradas, instrumentos y resultados se describen en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas del Departamento Administrativo de la Función Pública y como complemento en el DADEP se cuenta con el 127-PROVM-01 - Procedimiento administración de los riesgos y 127-FORVM-13 Formato MAPA DE RIESGOS INSTITUCIONALES para el desarrollo de la metodología.

No obstante, como anexo a la gestión del riesgo es necesario referenciar o tener en cuenta documentos técnicos que orientan esta gestión como el Manual Operativo del MIPG.

18. Actualización de las Matrices de Riesgos

La primera línea de defensa deberá monitorear permanentemente la efectividad de los controles establecidos para cada uno de los riesgos de su proceso, además de los eventos de riesgo que puedan afectar el cumplimiento de los objetivos también de su proceso, teniendo en cuenta factores como:

- Situaciones externas.
- Análisis de PQRS.
- Cambios en la normatividad.
- Gestión de activos de información.
- Evaluaciones y resultados de auditorías de entes de control externos.
- Resultados de auditorías internas.
- Eventos de riesgos materializados.
- Análisis y evaluación de resultados de indicadores de gestión.
- Relación con proveedores, grupos de interés y grupos de valor.

La actualización de las matrices de riesgos, estarán orientadas por los siguientes lineamientos:

- La verificación y actualización de los mapas de riesgos deberá realizarse por lo menos una vez al año para lo cual, los líderes de los procesos podrán solicitar apoyo a la Oficina Asesora de Planeación a través de mesas de trabajo.
- Las solicitudes de modificaciones de los mapas de riesgos por parte de los líderes de los procesos, deberán realizarse a través de correo electrónico indicando la justificación de la misma y en el caso en que la necesidad de modificación sea una conclusión de una mesa de trabajo con la Oficina Asesora de Planeación, el acta correspondiente deberá adjuntarse a la solicitud realizada por correo electrónico.
- Cada vez que exista la materialización de un riesgo identificado, el líder del proceso deberá evaluar la pertinencia de actualizarla, incluyendo el nivel de probabilidad que se afectará con la ocurrencia del evento.
- Las causales de eliminación de un riesgo son:
  - ✓ Que las causas que lo originaron desaparezcan.

- ✓ Que el servicio y/o la obligación objeto del riesgo, deje de ser competencia de la Defensoría del Espacio Público.
- ✓ Que por lo menos uno de los elementos del riesgo no corresponda a los criterios técnicos vigentes.
- ✓ Que el riesgo se encuentre identificado y gestionado en la matriz de otro tipo de riesgo.

- El control de cambios de las matrices de riesgos debe describir de manera clara, cada una de las modificaciones realizadas a cada uno de los riesgos.
- La Oficina Asesora de Planeación será la única dependencia autorizada para solicitar la publicación de las matrices de riesgos en la página web de la entidad, previa validación metodológica.

19. Control y Monitoreo (Periodo de revisión riesgos institucionales)

Los líderes de procesos realizan la revisión de los riesgos de manera permanente, pero informarán a la Oficina Asesora de Planeación de manera cuatrimestral, los avances obtenidos en los controles con las respectivas evidencias. Esta información deberá ser remitida a través de correo electrónico dentro de los cuatro (4) primeros días hábiles del mes siguiente al cuatrimestre finalizado para el caso de los riesgos de corrupción y dentro de los diez (10) primeros días hábiles del mes siguiente al cuatrimestre finalizado para los demás tipos de riesgos.

La Oficina Asesora de Planeación, en su calidad de segunda línea de defensa, realiza el monitoreo cuatrimestral con las evidencias aportadas por la primera línea de defensa y en el caso de los riesgos de corrupción, lo remitirá a la Oficina de Control Interno para la respectiva evaluación independiente dentro de los cuatro (4) días hábiles siguientes al vencimiento del plazo para el envío de la información por parte de la primera línea de defensa. En lo que corresponde al monitoreo de las matrices de los demás tipos de riesgos, la Oficina Asesora de Planeación deberá solicitar su publicación en la página web durante el mes siguiente a la finalización del cuatrimestre.

El monitoreo a los riesgos deberá realizarse cuatrimestral, con corte a 30 de abril, 31 de agosto y el 31 de diciembre.

El monitoreo debe incluir la actualización de los riesgos si se presentan cambios en el proceso que generen nuevos riesgos o se requieran modificar los factores determinantes que modifiquen la valoración de los riesgos identificados.

20. Términos y Definiciones

Accesibilidad: Acceso universal a la Web, independientemente del tipo de hardware, software, infraestructura de red, idioma, cultura, localización geográfica y capacidades de los usuarios (W3C World Wide Web Consortium). En el contexto colombiano, ha venido asumiéndose como las condiciones que se incorporan en sitios y herramientas web que favorecen el que usuarios en condiciones de deficiencia tecnológica, física o sensorial o en condiciones particulares de entornos difíciles o no apropiados, puedan hacer uso de estos recursos de la Web[1].

Aceptación de riesgo: Decisión generada por la entidad de aceptar las consecuencias y probabilidad de un riesgo en particular, sin adelantar acciones de reducción y control. La aceptación del riesgo también se deriva del nivel de riesgo o umbral en el cual el Departamento Administrativo de la Defensoría del Espacio Público acepta el riesgo.

Actitud (apetito) hacia el riesgo : Enfoque de la organización para evaluar y eventualmente buscar, retener, tomar o alejarse del riesgo.[2]

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

Activos de información: Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas…) que tenga valor para la organización.

Administración de riesgos: Proceso efectuado por la Alta Dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos. El enfoque de riesgos no se determina solamente con el uso de la metodología, sino logrando que la evaluación de los riesgos se convierta en una parte natural del proceso de planeación. (INTOSAI, 2000).

Amenaza: Causa Potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o una organización.[3]

Amenaza informática : Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio.[4]

Análisis cualitativo: Herramienta subjetiva que estandariza la evaluación de la probabilidad de ocurrencia y el impacto de los riesgos facilitando su evaluación y posibilidad de priorizarlos.

Análisis de riesgo: Uso sistemático de la información para identificar las fuentes y estimar el riesgo NTC-ISO /IEC 27001.

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

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

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

Causa inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa raíz 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.

Comunicación y consulta: Procesos continuos y reiterativos que una organización lleva a cabo para suministrar, compartir u obtener información e involucrarse en un diálogo con las partes interesadas, con respecto a la gestión del riesgo[5].

---

[1] MinTic. Glosario: Página Web https://www.mintic.gov.co/portal/604/w3-propertyvalue-1051.html. Actualizada el: 16 de octubre de 2018
[2] ICONTEC. NTC-ISO 31000: Norma técnica Gestión del riesgo Principios y Directrices. Numeral 2: Términos y definiciones Bogotá,2011 Página 5.
[3] Guía para la administración de los riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas Agosto-2018 V2. Página 9.
[4] Glosario del Mintic. Página Web https://www.mintic.gov.co/portal/604/w3-propertyvlue-1051.html.
[5] ICONTEC. NTC31000:2011. Gestión del Riesgo. Términos y Definiciones. Numeral 2.12 Bogotá, 2011. Página 4.

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

Consecuencia o impacto : Efectos generados por la ocurrencia de un riesgo que afecta los objetivos o un proceso de la entidad. Pueden ser entre otros, una pérdida, un daño, un perjuicio, un detrimento[6].

Control: Medidas que permiten minimizar la probabilidad de ocurrencia de un riesgo o el impacto producido ante su materialización, tales como procesos, procedimientos, políticas, entre otros.

Corrupción: Uso del poder para desviar la gestión de lo público hacia el beneficio privado.

Criterios para la evaluación de riesgos : Términos de referencia o parámetros con base en los cuales se evalúa la importancia de un riesgo. Los criterios para la evaluación del riesgo los establece la organización de acuerdo con sus necesidades y objetivos.

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

Evento: Presencia o cambio de un conjunto particular de circunstancias.[7] Dependiendo de las consecuencias o impactos que el evento pueda tener, se habla de que se materializa el riesgo para las situaciones en las cuales las consecuencias son negativas y se materializan las oportunidades cuando las consecuencias o impactos son positivos.

Factores de Riesgo: Son las fuentes generadoras de riesgos.

Identificación del riesgo. Proceso para encontrar, reconocer y describir el riesgo.[8]

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

Integridad: Propiedad de exactitud y completitud.

Mapa de riesgos : Es una herramienta, basada en los distintos sistemas de información, que pretende identificar las actividades o procesos sujetos a riesgo, cuantificar la probabilidad de estos eventos y medir el daño potencial asociado a su ocurrencia[9].

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

Política para la gestión del riesgo: Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.[10]

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 un (1) año.

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

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

Riesgo de trámites y otros procedimientos administrativos OPAs: Son los riesgos de corrupción asociados a trámites y OPA que se opera en Bogotá, teniendo en cuenta el universo de trámites distritales. En el caso de las entidades que realizan la identificación, la mayoría de ellas la hace de manera general asociada a la prestación de todos los trámites y servicios de la entidad, y no particular, es decir, considerando las características de cada uno de estos, sus relaciones con los grupos de valor y las debilidades del proceso que generan riesgos.

---

[6] Función Pública. Manual Técnico del Modelo Estándar de Control Interno para el Estado Colombiano -MECI- 2014. Página 64.
[7] ICONTEC. NTC-ISO 31000: Norma técnica Gestión del riesgo Principios y Directrices. Numeral 2: Términos y definiciones Bogotá, 2011 Página 21.
[8] ICONTEC. NTC-ISO 31000: Norma técnica Gestión del riesgo Principios y Directrices. Numeral 2: Términos y definiciones Bogotá, 2011 Página 6.
[9] Atlantic Review of Economics - 2nd Volume - 2013. Resumen. Página 2
[10] Norma Técnica Colombiana. NTC-ISO 31000: Gestión del riesgo Principios y Directrices. Página 5.

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

Riesgo del Sistema de Administración de Riesgo de Lavado de Activos y de la Financiación del Terrorismo – SARLAFT: Es el Sistema de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo, está compuesto por dos componentes. El componente de prevención del riesgo y el componente de control. La **prevención de riesgos** como su nombre lo indica, trata de prevenir que las entidades vigiladas sean utilizadas para dar apariencia de legalidad a recursos provenientes de actividades delictivas o, para la canalización de recursos hacia la realización de actividades terroristas. **El componente de control** es utilizado para detectar las operaciones que se pretendan realizar o se hayan realizado; durante este proceso se aplican medidas tanto preventivas como correctivas, con el fin de establecer los procedimientos del SARLAFT.

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.[11]

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

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

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

Tratamiento del riesgo: Proceso para modificar el riesgo. El tratamiento del riesgo puede implicar: Evitar el riesgo decidiendo no iniciar o continuar la actividad que lo originó, tomar o incrementar el riesgo con el fin de perseguir una oportunidad, retirar la fuente del riesgo, cambiar la probabilidad, cambiar las consecuencias, compartir el riesgo con una o varias de las partes (incluyendo los contratos y la financiación del riesgo) y retener el riesgo a través de la decisión informada. En ocasiones se hace referencia a los tratamientos del riesgo relacionados con consecuencias negativas como "mitigación del riesgo", "eliminación del riesgo", "prevención del riesgo" y "reducción del riesgo". El tratamiento del riesgo puede crear riesgos nuevos o modificar los existentes.[12]

Valoración del riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación del riesgo.[13]

Vulnerabilidad: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.[14]

Elaboró: Luis Fernando Arango Vargas - Profesional Oficina Asesora de Planeación
Revisó: Wisman Yesid Cotrino García, Jefe Oficina Asesora de Planeación.
Aprobó: Comité Institucional de Coordinación de Control Interno
Código de archivo: 150

CONTROL DE CAMBIOS		
VERSIÓN	FECHA	DESCRIPCIÓN DE MODIFICACIÓN
3	18/04/2024	Se ajustó el alcance de la política, se redefinió el capítulo 8. Sobre el compromiso de la política, conforme a Guía para la Administración del Riesgo y el diseño de controles en entidades públicas vigente del Departamento Administrativo de la Función Pública. Se eliminó la sección sobre la aceptación de riesgos de corrupción y se incluyeron los capítulos apetito y tolerancia al riesgo. Se actualizó el capítulo 15 sobre el accionar ante la materialización del riesgo. Se actualizó la periodicidad de la revisión de los riesgos por parte de las áreas Se ajustó la casilla responsable del cuadro línea estratégica pág. 11 Se ajustó la casilla Actividades a Realizar del cuadro Primera Línea de Defensa (se cambia Plan de Acción por acciones).

[11] Función Pública. Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. Versión 6, Página 12.
[12] ICONTEC. NTC-ISO 31000: Norma técnica Gestión del riesgo Principios y Directrices. Numeral 2: Términos y definiciones Bogotá, 2011 Página 8.
[13] ICONTEC. NTC-ISO 31000: Norma técnica Gestión del riesgo Principios y Directrices. Numeral 2: Términos y definiciones Bogotá, 2011 Página 6.
[14] Guía para la administración del riesgo y el diseño de controles en entidades públicas Octubre-2020 V5. Página 12 y 13.

CONTROL DE CAMBIOS		
VERSIÓN	FECHA	DESCRIPCIÓN DE MODIFICACIÓN
		Se ajustó la casilla Responsables y la casilla Actividades a realizar en el cuadro Segunda Línea de Defensa pág.12 Se actualiza el punto 8 Metodología y Normatividad Aplicable pág. 18. Se ajustó el numeral 11.2 Identificación de los activos de seguridad de la información pág. 28
4	24/12/2024	Se incluye el tipo de riesgo: Riesgo fiscal. Se ajustan algunos términos y definiciones. Se simplifica la política de administración del riesgo y en ella se incluyen los riesgos de tipo fiscal. Se ajustan la visión y los objetivos estratégicos de acuerdo con la nueva plataforma estratégica de la entidad. Se ajustan algunas responsabilidades y actividades de las líneas de defensa. Se incluye un numeral sobre la identificación del riesgo. Se incluye un numeral sobre la descripción del riesgo. Se incluye un numeral sobre la clasificación del riesgo. Se complementa el numeral de valoración del riesgo, incluyendo una descripción de sus cuatro etapas. Se incluyen lineamientos para los riesgos fiscales. Se incluyen más acciones a realizar ante la materialización de los riesgos y se identifican de acuerdo con el tipo de riesgo materializado. Se incluyen lineamientos para la actualización de las matrices de riesgos. Se establecen tiempos y lineamientos en lo que corresponde a control, monitoreo y comunicación de las matrices de riesgos.
5	26/05/2026	Se modifica el concepto de líneas de defensa, por líneas de responsabilidad Se modifica el capitulo 17, relacionado con las acciones ante la materialización definiendo el procedimiento ante esta situación tanto para los riesgos fiscales, de corrupción, gestión y seguridad digital. Se define la figura de oficial de cumplimiento para el componente de riesgos. Se ajusta la metodología de gestión de riesgos, en alineación con la Guía para la Gestión Integral del Riesgo en Entidades Públicas V.7