



ALCALDÍA MAYOR
DE BOGOTÁ D.C.

DEPARTAMENTO ADMINISTRATIVO DE LA
**DEFENSORÍA DEL
ESPACIO PÚBLICO**



Código SG/MIPG 127-PPVVM-02
Vigencia desde 02/03/2021
Versión 1

Política de Administración del Riesgo

Proceso
VERIFICACIÓN Y MEJORAMIENTO CONTINUO

Tabla de Contenido

1.	Introducción	4
2.	Términos y Definiciones	4
3.	Política de Administración del Riesgo.....	8
4.	Objetivos de la Política de Administración de Riesgos.....	9
4.1	Objetivo General de la Política de Administración de Riesgos del DADEP.....	9
4.2	Objetivo Específicos.....	9
5.	Alcance de la Política de Administración de Riesgos.....	9
6.	Roles y Responsabilidades en la Gestión del Riesgos.....	9
7.	Alineación de la Política con la Plataforma Estratégica de la Entidad	14
7.1	Misión:.....	14
7.2	Visión:.....	14
7.3	Objetivos Estratégicos:	15
7.4	Mapa de Procesos:	15
8.	Metodología y normatividad aplicable.....	16
9.	Establecimiento del contexto de la entidad	18
9.1	Factores del Contexto Externo que pueden afectar el funcionamiento del Departamento Administrativo de la Defensoría del Espacio Público.	19
9.2	Factores del Contexto Interno que pueden afectar el funcionamiento del Departamento Administrativo de la Defensoría del Espacio Público.	19
9.3	Factores del Contexto del Proceso que pueden afectar el funcionamiento del Departamento Administrativo de la Defensoría del Espacio Público.	20
10.	Niveles de Valoración del Riesgo para calificar la probabilidad y el impacto.....	20
11.	Niveles de aceptación al riesgo.....	24
11.1	Riesgos a Controlar – Administrar.....	25
11.2	Para los riesgos de gestión y seguridad digital se establece el siguiente nivel de aceptación:	25
10.2.1.	Riesgos a priorizar.....	25
11.3	Para los riesgos de corrupción se establece el siguiente nivel de aceptación.	25
11.4	Plan de Manejo de Riesgos	26



12.	Escenarios de pérdida de continuidad.....	26
13.	Etapas y Herramientas para la Gestión del Riesgo	27
14.	Control y Monitoreo (Periodo de revisión riesgos institucionales)	27
15.	Comunicación y Consulta.....	28

1. Introducción

Para el Departamento Administrativo de la Defensoría del Espacio Público – DADEP- es de vital importancia, lograr sus objetivos estratégicos, planes, proyectos y procesos institucionales a través de la realización de acciones soportadas en la prevención de los riesgos, implementado controles que promueven la generación de comportamientos éticos y conlleven a la construcción de una cultura de buen gobierno, que impida la materialización de riesgos de gestión, corrupción y seguridad digital.

Es así como el DADEP, con base en la normatividad vigente y la metodología establecida por el Departamento Administrativo de la Función Pública, diseña la política de gestión de riesgos como mecanismo para la fortalecer el control en los procesos que responda, a los acontecimientos potenciales o aquellos en los que puedan desencadenar situaciones de riesgo de gestión, corrupción o seguridad digital, en concordancia con las directrices en materia de gestión pública y el enfoque del Modelo de Planeación y Gestión- MIPG.

2. 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 Web¹.

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

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.

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 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.³

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

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

³ Glosario del Mintic. Página Web <https://www.mintic.gov.co/portal/604/w3-propertyvalue-1051.html>.

⁴ 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.

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 riesgo⁵.

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 detrimento⁶.

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 modifica al riesgo (Procesos, Política, dispositivos, prácticas u otras acciones).⁷

Control: Medida que permite reducir o mitigar un riesgo.

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.⁸ 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.⁹

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 ocurrencia¹⁰.

⁵ ICONTEC. NTC31000:2011. Gestión del Riesgo. Términos y Definiciones. Numeral 2.12 Bogotá, 2011. Página 4.

⁶ Función Pública. Manual Técnico del Modelo Estándar de Control Interno para el Estado Colombiano -MECI- 2014. Página 64.

⁷ 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.

⁸ ICONTEC. NTC-ISO 31000: Norma técnica Gestión del riesgo Principios y Directrices. Numeral 2: Términos y definiciones Bogotá, 2011 Página 21.

⁹ ICONTEC. NTC-ISO 31000: Norma técnica Gestión del riesgo Principios y Directrices. Numeral 2: Términos y definiciones Bogotá, 2011 Página 6.

¹⁰ Atlantic Review of Economics - 2nd Volume - 2013. Resumen. Página 2

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

Nivel de riesgo: Magnitud del riesgo, expresada en términos de la combinación de la probabilidad y las consecuencias o impacto que este tiene.

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

Política para la gestión del riesgo: Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.¹¹

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 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 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 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. Capacidad de riesgo: Es el

¹¹ Norma Técnica Colombiana. NTC-ISO 31000: Gestión del riesgo Principios y Directrices. Página 5.

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.

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

3. 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 y de Seguridad Digital, asociados a los objetivos estratégicos, planes, proyectos y procesos institucionales, considerando la metodología propia para su gestión, determinando los controles preventivos y detectivos oportunamente para evitar la materialización y la acción correctiva inmediata ante los eventos presentados, buscando con esto aceptar, reducir, evitar y compartir ante posible materialización las posibles consecuencias a fin de mantener los niveles de riesgo aceptables.

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.

4. Objetivos de la Política de Administración de Riesgos

4.1 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, los cuales harán énfasis en el fortalecimiento de los controles internos, con el fin de minimizar la probabilidad de materialización de cualquier tipo de riesgo que afecten el logro de las metas del Departamento.

4.2 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.
- 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.

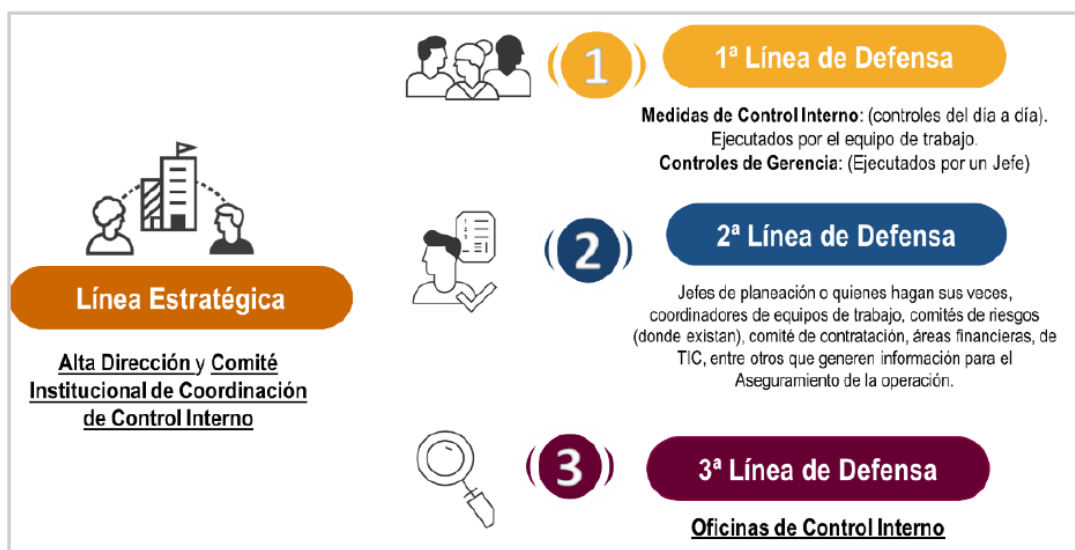
5. Alcance de la Política de Administración de Riesgos

La presente política aplica para todos y cada uno de los procesos institucionales, y los controles serán aplicados por todos los servidores públicos y contratistas del Departamento.

6. Roles y Responsabilidades en la Gestión del Riesgos

Con el fin de asegurar que las responsabilidades y autoridades para la gestión del riesgo se asignan y comunican a los roles pertinentes, el Departamento Administrativo de la Defensoría del Espacio Público determina las siguientes responsabilidades en relación con las líneas de defensa establecidas en el Modelo Integrado de Planeación y gestión MIPG:

Ilustración 1. Las Líneas de Defensa en el Modelo Estándar de Control Interno



Fuente: Manual Operativo del MIPG del DAFP 2019 V3.

Línea Estratégica	
Responsables	Equipo Directivo, Comité Institucional de Gestión y Desempeño; y el Comité Institucional de Coordinación de Control Interno.
Política, Identificación y Valoración del Riesgo	
Responsabilidades	- Definir y aprobar el marco general para la gestión del riesgo, la gestión de la continuidad del negocio y el control. - Analizar los riesgos, vulnerabilidades, amenazas y escenarios de pérdida de continuidad de negocio institucionales que pongan en peligro el cumplimiento de los objetivos estratégicos, planes institucionales, metas, compromisos de la entidad y capacidades para prestar servicios. - Definir y aprobar la política para la administración del riesgo. - Garantizar el cumplimiento de los planes de la entidad.
Actividades a Realizar	
- Establecer la política de gestión de riesgos de la entidad. - Definir los niveles de aceptación de riesgos. - Establece la periodicidad del monitoreo y seguimiento. - Supervisa el cumplimiento de cada una de las etapas de la gestión de riesgos. - Revisar los cambios en el Direccionamiento estratégico o en el entorno y como estos puedan generar nuevos riesgos o modificar los existentes. - Revisar los planes de acción establecidos en los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar la posible repetición del evento.	
Comunicación y Consulta	
Corresponde al Comité Institucional de Coordinación de Control Interno establecer la Política de Gestión de Riesgos y asegurarse de su permeabilización en todos los niveles de la organización pública,	

de tal forma que se conozcan claramente los niveles de responsabilidad y autoridad que posee cada una de las tres líneas de defensa frente a la gestión del riesgo.

Accionar Ante la Materialización del Riesgo de Corrupción

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

Primera Línea de Defensa

Responsables Líderes de Proceso y Responsable de Proyecto

Política, Identificación y Valoración del Riesgo

Responsabilidades	- Desarrollar e implementar procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora. - Orientar el desarrollo e implementación de políticas y procedimientos internos y asegurar que sean compatibles con las metas y objetivos de la entidad y emprender las acciones de mejoramiento para su logro. - Informar a la Oficina Asesora de Planeación (segunda línea) sobre los riesgos materializados en los objetivos, programas, proyectos y planes de los procesos a cargo. - Asegurar que al interior de su grupo de trabajo se reconozca el concepto de "administración del riesgo", la política y la metodología definida, los actores y el entorno del proceso aprobados por la primera línea de defensa.
--------------------------	---

Actividades a Realizar

- Delegar, por parte del líder del proceso, el (los) profesionales que se encargarán de la identificación, monitoreo, reporte y socialización del riesgo asociados.
- Revisar los cambios en el Direccionamiento estratégico o en el entorno y como estos puedan generar nuevos riesgos o modificar los existentes.
- Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos.
- Revisar el adecuado diseño y ejecución de los controles establecidos para la mitigación de riesgos.
- Revisar el cumplimiento de los objetivos de sus procesos y sus indicadores de desempeño, e identificar los posibles riesgos que se están materializando.
- Revisar y reportar a planeación, lo eventos de riesgos que se han materializado en la entidad.
- Revisar los planes de acción establecidos en los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar la posible repetición del evento.
- Revisar y hacer seguimiento al cumplimiento de las actividades y planes de acción acordados con la línea estratégica, segunda y tercera línea de defensa en relación con la gestión de riesgos.
- Reportar los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos.

Comunicación y Consulta

- Asegurarse de implementar la metodología para mitigar los riesgos en la operación, reportando a la segunda línea sus avances y dificultades.
- Divulgar y sensibilizar al interior de sus dependencias el mapa de riesgos junto con el plan de manejo y políticas de operación que se derivan.

Accionar Ante la Materialización del Riesgo de Corrupción

- Informar al Proceso de Direccionamiento Estratégico sobre el hecho encontrado.
- Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante la instancia de control correspondiente.

- Proceder de manera inmediata a aplicar el plan de contingencia (si lo hay) que permita la continuidad del servicio o el restablecimiento de este (si es el caso), documental en el Plan de mejoramiento.
- Iniciar el análisis de causas y determinar acciones preventivas y de mejora, documentar en el Plan de Mejoramiento Institucional y verificar la calificación y ubicación del riesgo para su inclusión en el mapa de riesgos.
- Analizar y actualizar los riesgos del proceso.

Segunda Línea de Defensa

Responsables	Jefe de la Oficina Asesora de planeación, supervisores e interventores de contratos o proyectos.
---------------------	--

Política, Identificación y Valoración del Riesgo

Responsabilidades	• Asegurar que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende. • Monitorear la gestión de riesgo y control ejecutada por la primera línea de defensa, complementando su trabajo.
--------------------------	--

Actividades a Realizar

- Revisar los cambios en el direccionamiento estratégico o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de solicitar y apoyar en la actualización de las matrices de riesgos.
- Revisar la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar.
- Revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y determinar las recomendaciones y seguimiento para el fortalecimiento de estos.
- Revisar el perfil de riesgo inherente y residual por cada proceso y consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad.
- Realizar seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos.
- Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelva a materializar el riesgo y lograr el cumplimiento a los objetivos.
- Realizar el monitoreo a los riesgos en la periodicidad establecida.

Comunicación Y Consulta

- Difundir y asesorar a la primera línea de defensa en la metodología, así como de los planes de tratamiento de riesgo identificados en todos los niveles de la entidad, de tal forma que se asegure su implementación.
- Impulsar a nivel institucional una cultura de gestión del riesgo, a través de capacitaciones, mesas de trabajo y asesorías, con el fin de mejorar el conocimiento y apropiación del enfoque basado en riesgos.
- Consolidar el Mapa de Riesgos de la entidad.
- Divulgar del Mapa de Riesgos de Corrupción a partes interesadas y comunidad en general a través de su publicación en la página web de la Entidad.

Accionar Ante la Materialización del Riesgo de Corrupción

- Asesorar a la primera línea de defensa en el análisis de causas y la determinar acciones preventivas y de mejora, documentar en el Plan de Mejoramiento Institucional.
- Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelva a materializar el riesgo y lograr el cumplimiento a los objetivos.
- Actualizar el mapa de riesgos, con la información reportada por la primera línea de defensa.

Tercera Línea de Defensa

Responsables Oficina de Control Interno

Política, Identificación Y Valoración Del Riesgo

Responsabilidades

- Proporcionar información sobre la efectividad de la entidad en la gestión, a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa
- Proporcionar un aseguramiento basado en el más alto nivel de independencia y objetividad sobre la efectividad del S.C.I.
- Proporcionar aseguramiento objetivo en las temas identificadas no cubiertas por la segunda línea de defensa.
- Recomendar mejoras a la política de operación para la administración del riesgo

Actividades a Realizar

- Asesorar a la primera línea de defensa de forma coordinada con la Oficina **Asesora** de Planeación, en la metodología e identificación de los riesgos y diseño de controles.
- Revisar los cambios en el “Direccionamiento estratégico” o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables.
- Revisión de la adecuada definición de los objetivos institucionales a los objetivos de los procesos que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar.
- Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos, además de incluir los riesgos de corrupción.
- Revisar el adecuado diseño y ejecución de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de estos.
- Revisar el perfil de riesgo inherente y residual por cada proceso consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad o que su calificación del impacto o probabilidad del riesgo no es coherente con los resultados de las auditorías realizadas.
- Para mitigar los riesgos de los procesos estos se deben encontrar documentados y actualizados en los procedimientos y los planes de mejora como resultado de las auditorías efectuadas, además, se lleven a cabo de manera oportuna, estableciendo la causa raíz del problema y buscando evitarse en lo posible, la repetición de hallazgos y la materialización de los riesgos.

Comunicación y Consulta

- Impulsar a nivel institucional una cultura de gestión del riesgo, a través de capacitaciones, mesas de trabajo y asesorías, con el fin de mejorar el conocimiento y apropiación del enfoque basado en riesgos.
- Informar sobre la efectividad de la entidad en la gestión a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa.

Accionar Ante la Materialización del Riesgo de Corrupción

- Informar al líder del proceso sobre el hecho.
- Informar a la segunda línea de defensa con el fin facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos.
- Acompañar al líder del proceso en la revisión, análisis y toma de acciones correspondientes para resolver el hecho.
- Verificar que se tomaron las acciones y se actualizó el mapa de riesgos correspondiente.

7. 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 definida en el artículo 3 "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.

7.1 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.

7.2 Visión:

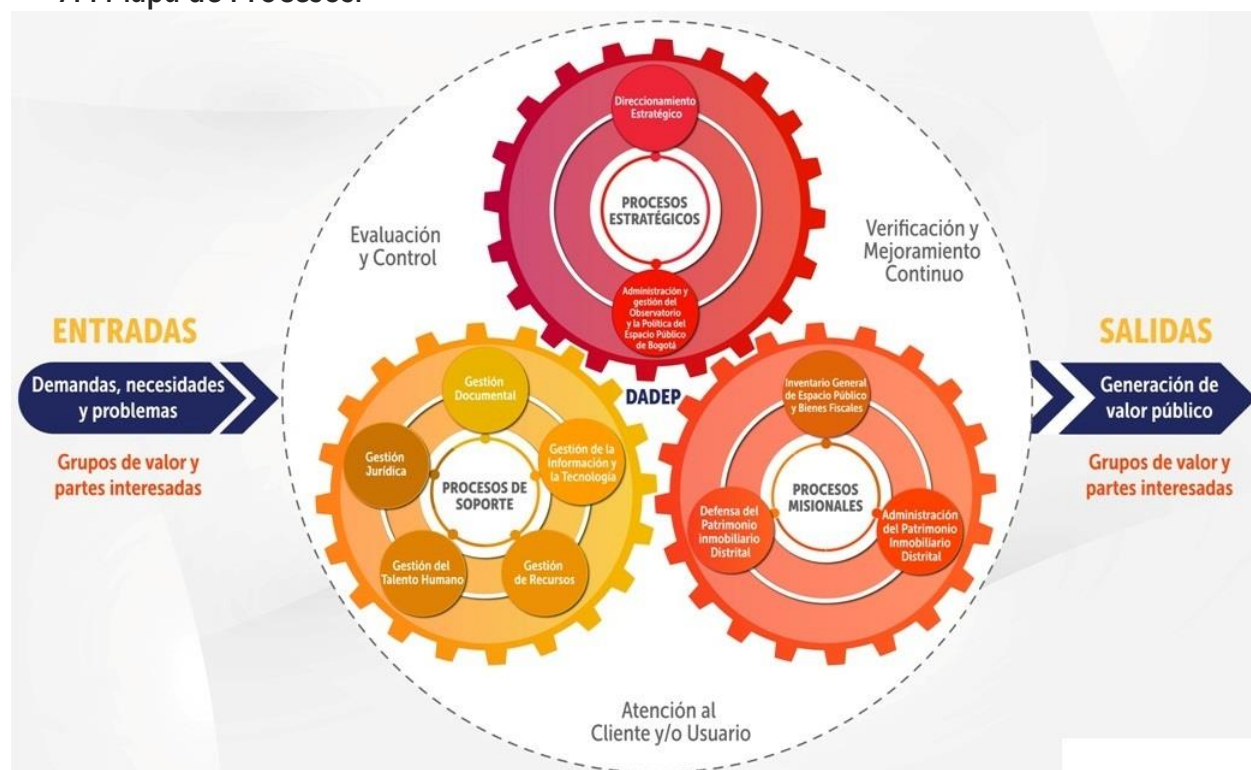
En 2024 el Departamento Administrativo de la Defensoría del Espacio Público será una entidad reconocida a nivel distrital y nacional como líder en la protección integral del espacio público y del patrimonio inmobiliario distrital, la gestión del conocimiento urbanístico de los bienes de

uso público y fiscales del nivel central de Bogotá, y por promover la participación ciudadana, la corresponsabilidad y la coordinación interinstitucional.

7.3 Objetivos Estratégicos:

- Contribuir al incremento del uso, goce y disfrute del patrimonio inmobiliario distrital y el espacio público, con acceso universal a la ciudadanía.
- Aumentar la oferta cuantitativa, cualitativa y la equidad territorial del patrimonio inmobiliario distrital y el espacio público.
- Mejorar la coordinación interinstitucional con todas las entidades que tienen competencia en materia de espacio público, así como la comunicación con los grupos de interés y de valor.
- Fortalecer la capacidad institucional en el marco del Modelo Integrado de Planeación y Gestión, bajo los enfoques de una gestión orientada a resultados, la eficiencia en el manejo de recursos, la transparencia, el gobierno abierto y la participación de los grupos de interés.

7.4 Mapa de Procesos:



Por lo tanto, dentro de los aspectos que el DADEP tiene en cuenta para la identificación de los riesgos esta:

Ilustración 2. Conocimiento y análisis de la entidad



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades Públicas del DAFP 2020 V5.

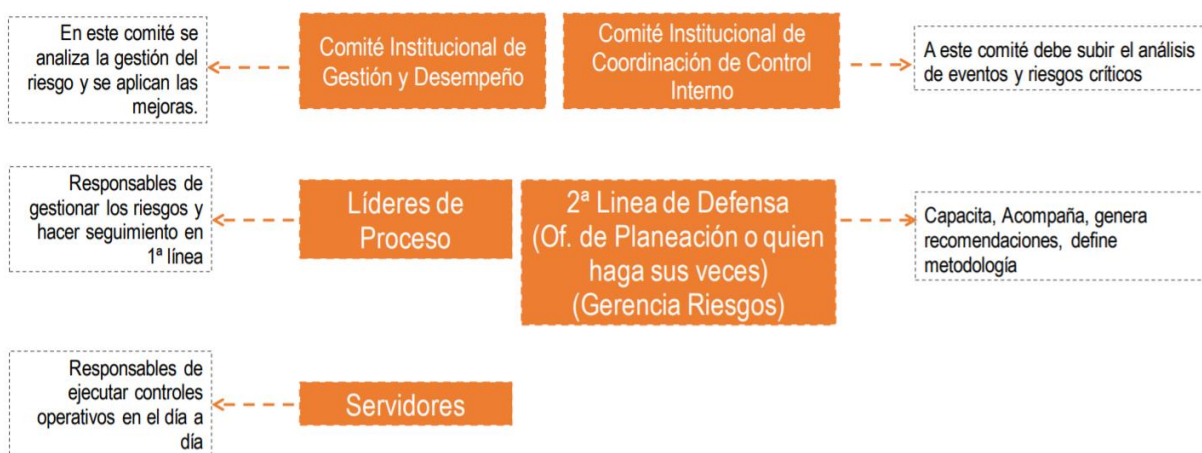
8. Metodología y normatividad aplicable

El Departamento Administrativo de la Defensoría del Espacio Público, aplicará la metodología establecida por el Departamento Administrativo de la Función Pública, descrita en la Guía para la administración de los riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas.

Así mismo, se aplicarán los lineamientos del Modelo Integrado de Planeación y Gestión MIPG- Según lo contemplado en la normatividad vigente, principalmente el Decreto 1499 de 2017, la Guía para Elaborar el Mapa de Aseguramiento en las Entidades del Distrito de la Secretaria General y el Decreto Distrital 807 de 2019 "Por medio del cual se reglamenta el Sistema de Gestión en el Distrito Capital y se dictan otras disposiciones"

El modelo integrado de planeación y gestión (MIPG) define para su para su operación articulada la creación en todas las entidades del Comité Institucional de Gestión y Desempeño y el Comité Institucional de Coordinación de Control Interno en este marco general, para una adecuada gestión del riesgo, dicha institucionalidad entra a funcionar de la siguiente forma:

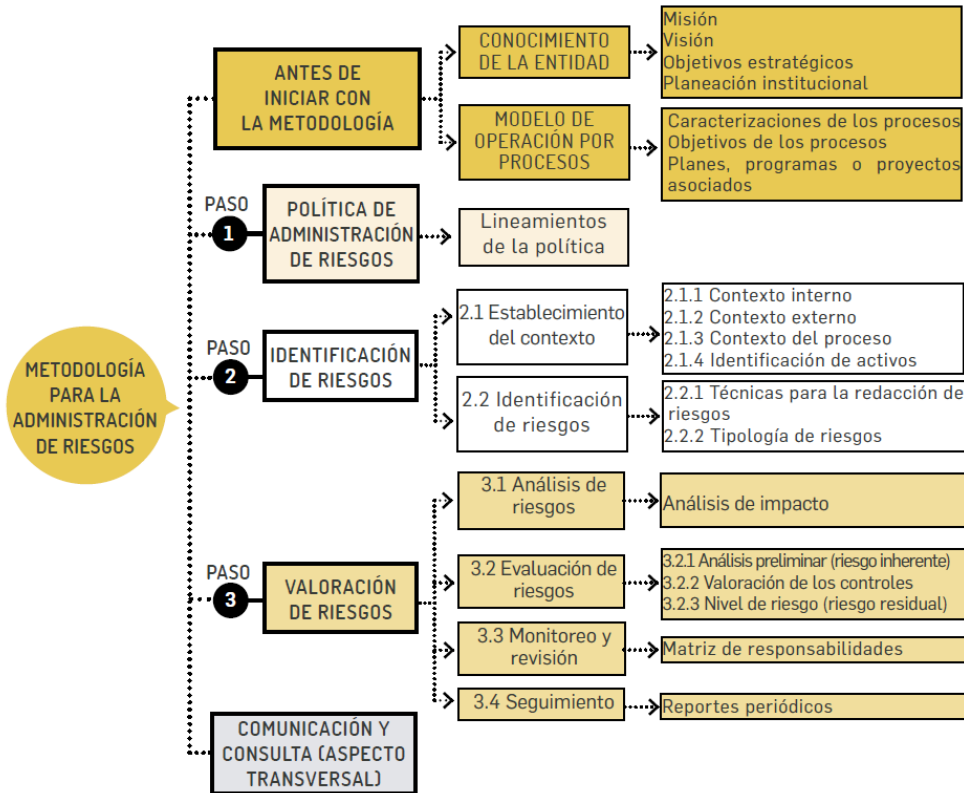
Ilustración 3. Operatividad Institucionalidad para la Administración del Riesgo



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades Públicas del DAFP 2020 V5.

La metodología para la administración del riesgo requiere de un análisis inicial relacionado con el estado actual de la estructura de riesgos y su gestión en la entidad, además del conocimiento de esta desde un punto de vista estratégico de la aplicación de los tres (3) pasos básicos para su desarrollo y, finalmente, de la definición e implantación de estrategias de comunicación transversales a toda la entidad para que su efectividad pueda ser evidenciada, como se muestra a continuación:

Ilustración 4, Metodología para la administración del riesgo



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

9. 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, esto permite conocer y entender la entidad y su entorno, lo que determinará 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 organización, para ello se debe tener en cuenta el contexto estratégico en el que opera la entidad, 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 el DADEP son los siguientes:

9.1 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 o para el proyecto 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, energía, 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, Manejo de residuos y Contribución al desarrollo sostenible

Legales y Reglamentarios: Normatividad externa (leyes, decretos, ordenanzas y acuerdos). Nuevas disposiciones legales que afecten a la Entidad (laborales, contratación, manejo de espacio público, sectoriales).

9.2 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.

9.3 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 digital del proceso: información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso, como de cara al ciudadano. Ver conceptos básicos relacionados con el riesgo páginas 8 y 9.

10. Niveles de Valoración del Riesgo para calificar la probabilidad y el impacto

Con el fin de poder determinar la posibilidad de ocurrencia de un riesgo, se adoptan los siguientes criterios para clasificar la probabilidad de riesgo en el DADEP.

Ilustración 5. Criterios para definir el nivel de probabilidad

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 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, se adoptan los siguientes criterios para calificar el impacto

Ilustración 6. Criterios para definir el nivel de impacto

IMPACTO DE GESTIÓN		
Niveles para calificar el impacto	Impacto (consecuencias) Cuantitativo	Impacto (consecuencias) Cualitativo
5 Catastrófico	- Impacto que afecte la EJECUCIÓN presupuestal en un valor $\geq 50\%$ - Pérdida de cobertura en la prestación de los servicios de la entidad $\geq 50\%$. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor $\geq 50\%$ - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor $\geq 50\%$ del presupuesto general de la entidad.	- Interrupción de las operaciones de la Entidad por más de cinco (5) días. - Intervención por parte de un ente de control u otro ente regulador. - Pérdida de Información crítica para la entidad que no se puede recuperar. - Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. - Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.
4 Mayor	- Impacto que afecte la ejecución presupuestal en un valor $\geq 20\%$ - Pérdida de cobertura en la prestación de los servicios de la entidad $\geq 20\%$. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor $\geq 20\%$ - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor $\geq 20\%$ del presupuesto general de la entidad.	- Interrupción de las operaciones de la Entidad por más de dos (2) días. - Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. - Sanción por parte de ente de control u otro ente regulador. - Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. - Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos
3 Moderado	- Impacto que afecte la EJECUCIÓN presupuestal en un valor $\geq 5\%$	- Interrupción de las operaciones de la Entidad por un (1) día.

IMPACTO DE GESTIÓN		
Niveles para calificar el impacto	Impacto (consecuencias) Cuantitativo	Impacto (consecuencias) Cualitativo
	- Pérdida de cobertura en la prestación de los servicios de la entidad $\geq 10\%$. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor $\geq 5\%$ - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor $\geq 5\%$ del presupuesto general de la entidad.	- Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. - Inoportunidad en la información ocasionando retrasos en la atención a los usuarios. - Reproceso de actividades y aumento de carga operativa. - Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. - Investigaciones penales, fiscales o disciplinarias.
2	Menor - Impacto que afecte la ejecución presupuestal en un valor $\leq 1\%$ - Pérdida de cobertura en la prestación de los servicios de la entidad $\leq 5\%$. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor $\geq 1\%$ - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor $\geq 1\%$ del presupuesto general de la entidad.	- Interrupción de las operaciones de la Entidad por algunas horas. - Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias. - Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.
1	Insignificante - Impacto que afecte la ejecución presupuestal en un valor $\geq 0,5\%$ - Pérdida de cobertura en la prestación de los servicios de la entidad $\geq 1\%$. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor $\geq 0,5\%$ - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor $\geq 0,5\%$ del presupuesto general de la entidad.	- No hay interrupción de las operaciones de la entidad. - No se generan sanciones económicas o administrativas. - No se afecta la imagen institucional de forma significativa.

Fuente: 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, 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 7. Mapa de Calor

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)	Calificación 1 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

Ilustración 8. Medición de impacto de riesgos de Corrupción

IMPACTO CORRUPCIÓN			
NOMBRE DEL RIESGO DE CORRUPCIÓN			
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?		
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

Ilustración 9. Valoración de impacto de Riesgos Seguridad Digital

Nivel	Valor del Impacto	Impacto (Consecuencias) Cuantitativo	Impacto (Consecuencias) Cualitativo
CATASTRÓFICO	5	Afectación en un valor $\geq 50\%$ de la población. Afectación en un valor $\geq 50\%$ 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 $\geq 20\%$ e inferior al 50% de la población. Afectación en un valor $\geq 20\%$ 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 $\geq 10\%$ y menor al 20% de la población. Afectación en un valor $\geq 10\%$ 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 $\geq 1\%$ y menor al 10% de la población. Afectación en un valor $\geq 1\%$ 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

11. Niveles de aceptación al riesgo

La gestión del riesgo en la Defensoría del Espacio Público 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:

11.1 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 teniendo en cuenta los siguientes lineamientos:

11.2 Para los riesgos de gestión y seguridad digital se establece el siguiente nivel de aceptación:

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

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

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

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

Los riesgos identificados se deben incluir en el mapa de riesgos Institucional y se les realizará monitoreo cada cuatro (4) meses.

10.2.1. Riesgos a priorizar

Los riesgos ubicados en la zona de riesgo extrema y alta serán atendidos a través de acciones concretas. En todo caso, se tendrá como referencia el análisis costo/beneficio para el manejo o la administración del riesgo.

11.3 Para los riesgos de corrupción se establece el siguiente nivel de aceptación.

Zona de riesgo **BAJA**: Ningún riesgo de corrupción podrá ser aceptado.

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

Zona de riesgo **ALTA y EXTREMA** Se adoptan medidas para:

- Reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles.

- Evitar Se abandonan las actividades que dan lugar al riesgo, decidiendo no iniciar o no continuar con la actividad que causa el riesgo.
- Transferir o compartir una parte del riesgo para reducir la probabilidad o el impacto de este.

Periodicidad cuatrimestral de seguimiento para evitar su materialización por parte de los procesos a cargo de estos.

De igual manera 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.

11.4 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.

12. 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:

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.
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 de los 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.
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.

13. Etapas y Herramientas para la Gestión del Riesgo

La gestión de riesgos comprende las actividades de análisis del contexto interno y externo, identificación y análisis del riesgo, valoración, evaluación, definición de controles para el tratamiento y seguimiento. 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 DAFP 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 con documentos técnicos que orientan esta gestión como el Manual Operativo del MIPG.

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

El control y monitoreo de riesgos en el DADEP se realizará:

- En primera instancia por el responsable o líder del proceso y
- En instancias posteriores por las auditorías internas programadas por la Oficina de Control Interno.

La finalidad principal de éstas es verificar las disposiciones de monitoreo y sugerir los correctivos u oportunidades de mejora para los ajustes necesarios a los riesgos identificados.

El monitoreo a los riesgos deberá realizarse cuatrimestral, con corte a 30 de abril, 31 de agosto y el 31 de diciembre, durante los 10 primeros días hábiles contados a partir de dichas fechas de corte.

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.

15. Comunicación y Consulta

La administración del riesgo debe ser un tema conocido por todos los funcionarios públicos y contratistas del Departamento Administrativo de la Defensoría del Espacio Público, para lo cual se utilizarán los medios de comunicación virtuales y presenciales. Los mapas de riesgos de la entidad se publicarán conforme indique la normatividad vigente, en el visor del Modelo Integrado de Planeación y Gestión - MIPG sgc.dadep.gov.co y en la página Web de la entidad www.dadep.gov.co.

Elaboró: Luis Fernando Arango Vargas. Profesional Oficina Asesora de Planeación y Alexander Oliveros Paredes, Contratista.

Revisó: Alejandra Jaramillo Fernández, Jefe Oficina Asesora de Planeación.

Aprobó: Comité Institucional de Coordinación de Control Interno. 03/02/2021

Código de archivo: 140-155-5



CONTROL DE CAMBIOS		
VERSIÓN	FECHA	DESCRIPCIÓN DE MODIFICACIÓN
1	29/01/2021	Actualización de acuerdo con la guía de riesgos del Departamento Administrativo de la Función Pública -diciembre 2020; esta política se encontraba en el proceso de Direccionamiento Estratégico por lo que cuenta con dos versiones anteriores en este proceso.