Política de Administración del Riesgo

Código SG/MIPG	127-PPPVM-02
Vigencia desde	24/12/2024
Versión	04

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. 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.

[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.

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].

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

[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.

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]

[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.

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.

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.

[11] Función Pública. Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. Versión 6, Página 12.

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]

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, 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.

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, 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.

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 y/o con un impacto fiscal.

[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.

- 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.

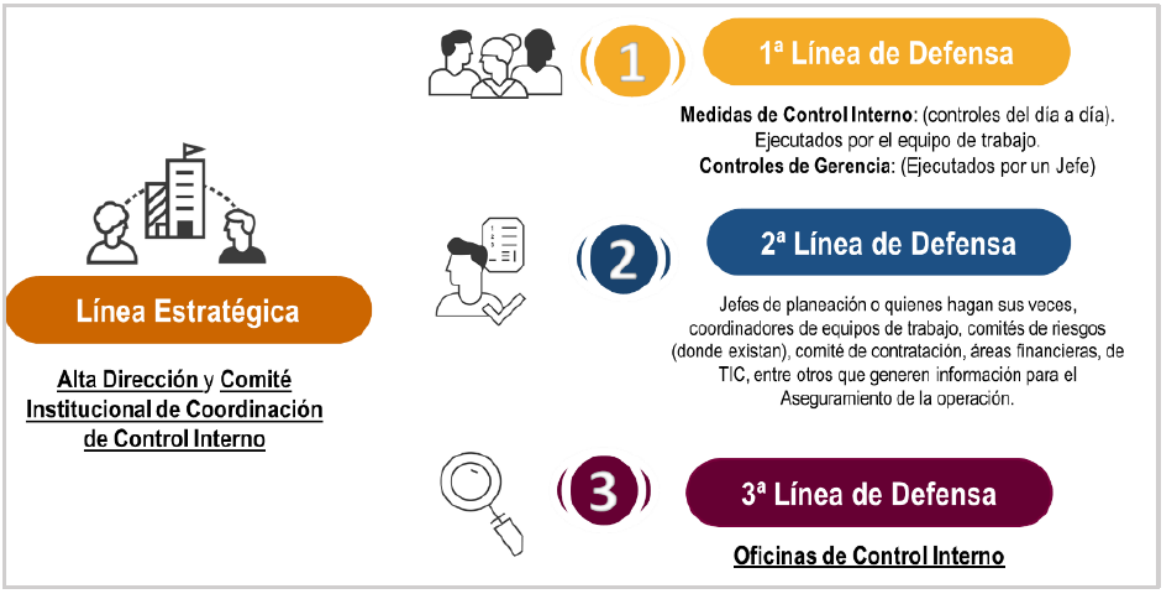
5. Alcance de la Política de Administración de Riesgos

La 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.

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 asignen y comuniquen 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

Línea Estratégica	
Responsables	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. – Establecer la periodicidad del monitoreo y seguimiento. – Supervisar 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 cómo estos puedan generar nuevos riesgos o modificar los existentes. – Revisar las acciones 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 aprobar 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 las acciones establecidas 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 Responsables 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 asociado. – 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 la oficina asesora de planeación, los eventos de riesgos que se han materializado en la entidad. – Revisar las acciones establecidas 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 acciones 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, incluida la materialización de alguno de ellos. – 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. – Para mitigar los riesgos de los procesos, éstos se deben encontrar documentados y actualizados en los procedimientos y los planes de mejora como resultado de las auditorías efectuadas, además, se deben llevar a cabo de manera oportuna, estableciendo la causa raíz del problema y buscando evitar en lo posible, la repetición de hallazgos y la materialización de los riesgos.

Segunda Línea de Defensa	
Responsables	Jefe de la Oficina Asesora de planeación, supervisores de contratos
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 e identificar cómo estos pueden 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 esté por fuera del perfil de riesgo de la entidad. – Realizar seguimiento a las actividades de control establecidas para la mitigación de los riesgos de los procesos que se encuentren documentadas y actualizadas en los procedimientos. – Revisar las acciones establecidas 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 en la determinación de 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 los temas identificados no cubiertos 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. – Evaluar los cambios en el “Direccionamiento Estratégico” o en el entorno y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables.	

– Evaluar 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. – Evaluar 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. – Evaluar 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 esté por fuera del perfil de riesgo de la entidad o que su calificación del impacto o probabilidad no sea coherente con los resultados de las auditorías realizadas.
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 de 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 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.

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 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.

7.3 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.

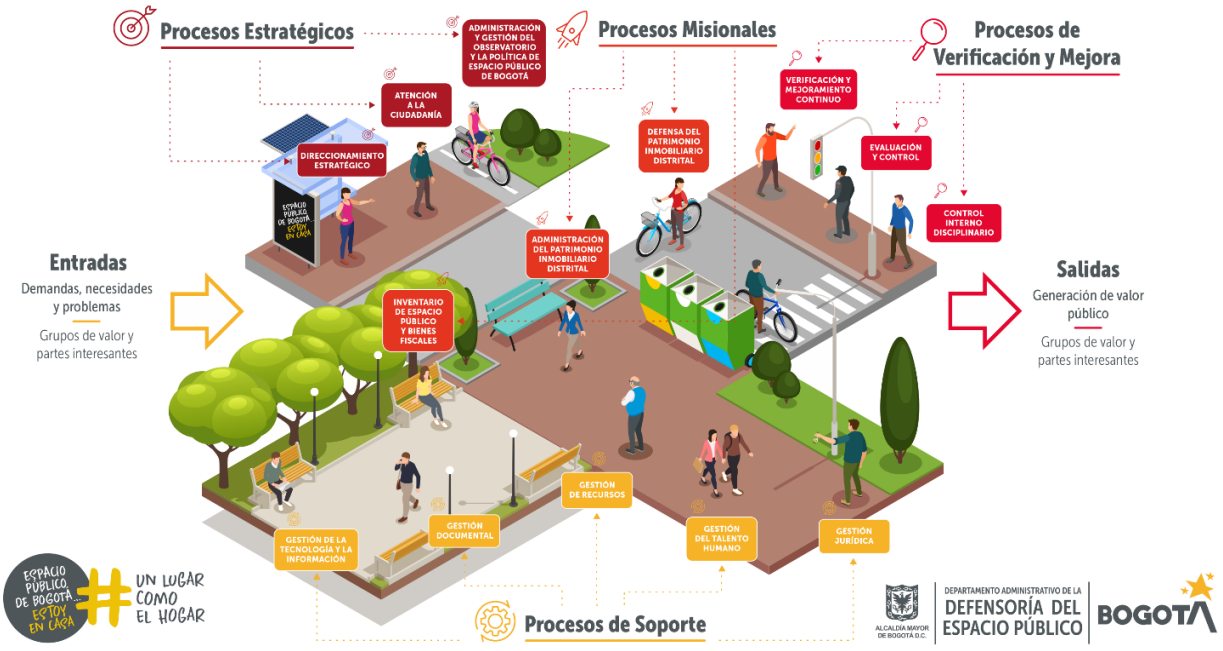
2.Aumentar la oferta cualitativa y cuantitativa de espacio público inclusivo y seguro, con enfoque de género, poblacional, étnico y diferencial.

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.

7.4 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:

Ilustración 3. Conocimiento y análisis de la entidad

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

8. 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.

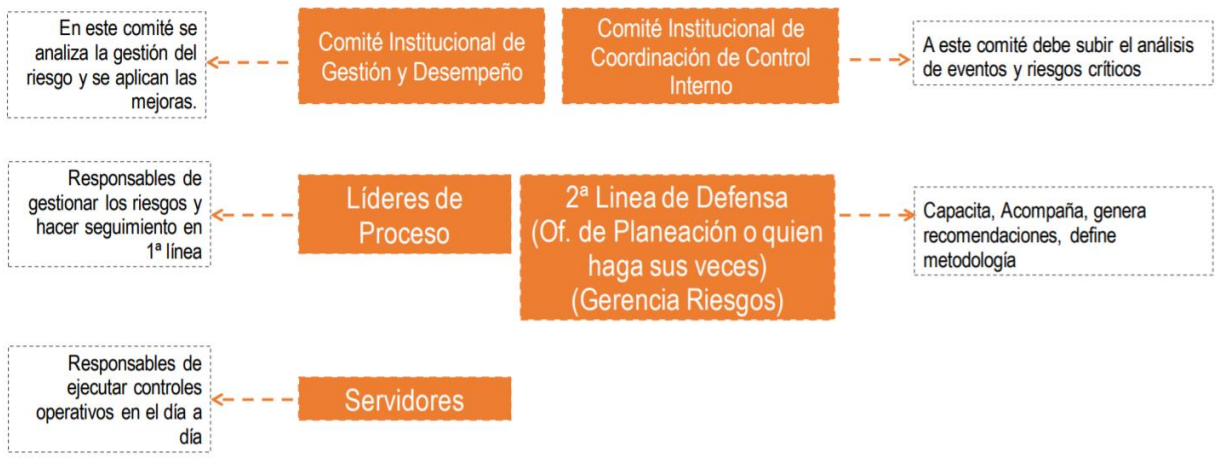
9. Metodología y Normatividad Aplicable

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 del Riesgo 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 Secretaría General y el Decreto Distrital 221 de 2023 “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 operación articulada, la creación en todas las entidades del Comité Institucional de Gestión y Desempeño y el Comité Institucional de Coordinación de Control Interno y para una adecuada gestión del riesgo, dicha institucionalidad entra a funcionar de la siguiente forma:

Ilustración 4. Operatividad Institucionalidad para la Administración del Riesgo

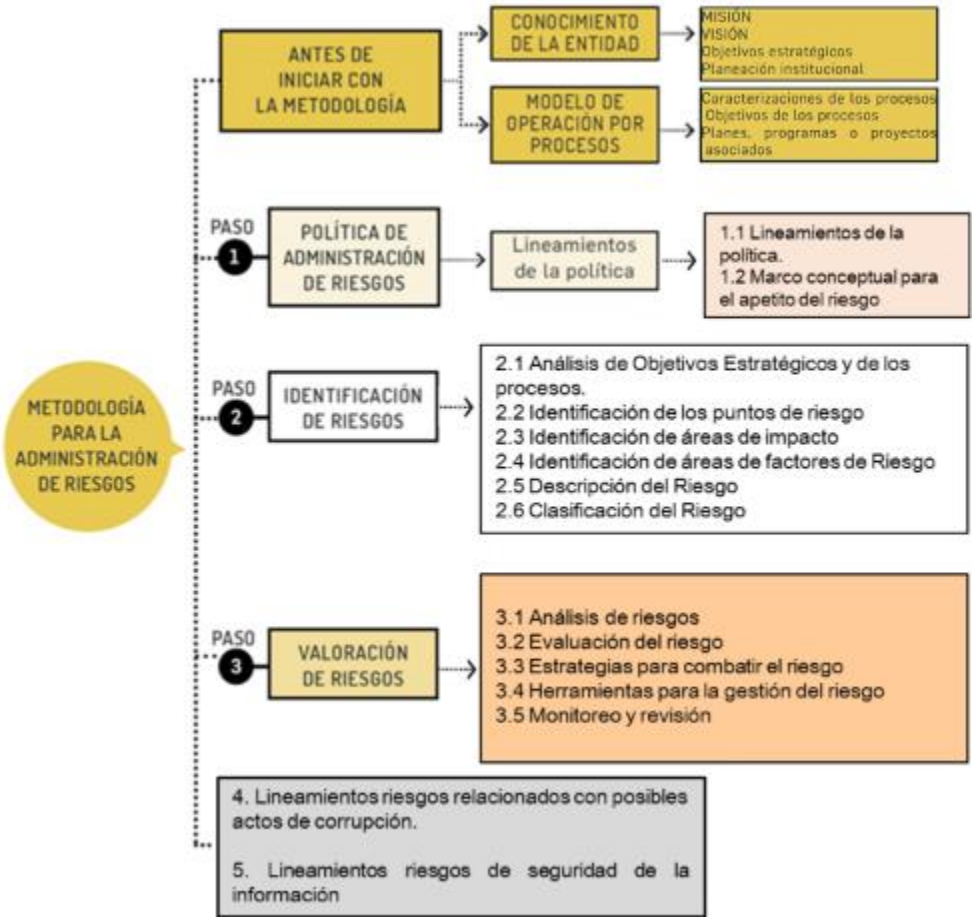


Fuente: Guía para la administración del riesgo y el diseño de controles en entidades Públicas del DAFP

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 ésta 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 5. Metodología para la administración del riesgo



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

10. 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.

10.1. 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:

10.2. 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.

10.3. 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.

10.4. 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.

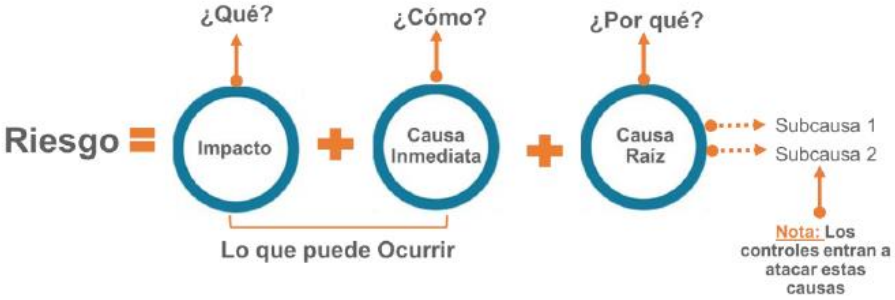
Activos de seguridad de la información del proceso: información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso.

10.5. 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 6. Estructura de la redacción del riesgo



Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas del Departamento Administrativo de la Función Pública

10.6. 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:

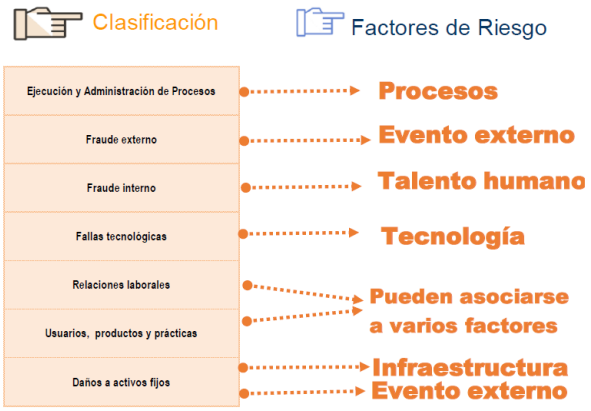
Ilustración 7. Categorías de los riesgos

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 y el Diseño de Controles en Entidades públicas del Departamento Administrativo de la Función Pública

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 8. Relación entre factores y clasificación del riesgo



Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades públicas del Departamento Administrativo de la Función Pública

11. 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

11.1. 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 9. 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 10. 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
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

11.2. 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 11. Mapa de Calor

Matriz de Calor Inherente		Impacto				
Probabilidad	Muy Alta 100%					
	Alta 80%					
	Media 60%					
	Baja 40%					
	Muy Baja 20%					
		Leve 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%

Extremo
Alto
Moderado
Bajo

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.

11.2.1. 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.

12. 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).

12.1. 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.

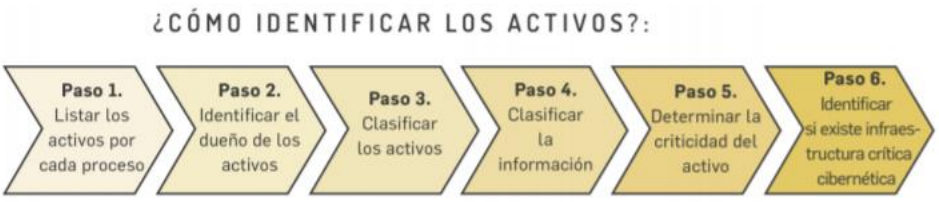
Ilustración 2. Identificación activos de información.

¿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).
-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 3. 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 4. 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

12.2. 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 5. 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

12.3. 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 16. Valoración de impacto de Riesgos Seguridad de la Información

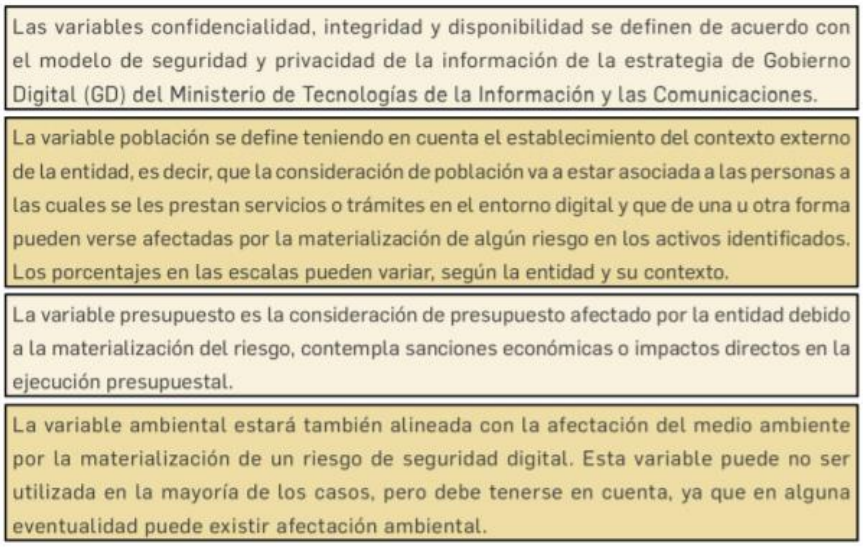
Nivel	Valor del Impacto	Impacto (Consecuencias) Cuantitativo	Impacto (Consecuencias) Cualitativo
CATASTRÓFICO	5	Afectación en un valor ≥ 50% de la población. Afectación en un valor ≥ 50% del presupuesto anual de la entidad Afectación muy grave del medio ambiente que requiere ≥ 3 años de recuperación.	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.

Nivel	Valor del Impacto	Impacto (Consecuencias) Cuantitativo	Impacto (Consecuencias) Cualitativo
			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 17. Variables a tener en cuenta para la valoración de los riesgos de seguridad de la información



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

12.4. 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 18. 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

13. 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.

13.1. 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

13.2. 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 19. 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 20. 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?		
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 21. 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

14. Lineamientos para los Riesgos Fiscales

14.1. 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.

14.2. 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

15. 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:

15.1. 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.

15.2. 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.

15.3. 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.

15.4. 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.

16. 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.
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.

17. Acciones ante los riesgos materializados

A continuación, se establecen los responsables y las acciones de respuesta a adelantar para cuando se materializan riesgos identificados en la matriz de riesgos.

Líder de proceso debe:

✓ Riesgos Fiscales y de Corrupción:

- Informar al líder del proceso de Direccionamiento Estratégico y al Comité Institucional de Gestión y Desempeño sobre el hecho encontrado.
- Tramitar la denuncia ante la instancia judicial y/o de control correspondiente, dependiendo del riesgo materializado.
- Identificar las acciones correctivas necesarias y documentarlas en el Plan de mejoramiento.
- Efectuar el análisis de causas y determinar acciones preventivas y de mejora.
- Actualizar el mapa de riesgos.

✓ Riesgos de Gestión por proceso:

- Informar al proceso de Direccionamiento Estratégico y al Comité Institucional de Gestión y Desempeño sobre el riesgo materializado.
- 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.

✓ Riesgos de Seguridad de la información:

- Aplicar de manera inmediata el Plan de Contingencia o de tratamiento de incidentes de seguridad de la información que permita la continuidad del servicio o el restablecimiento del mismo.
- Iniciar el análisis de causas y determinar acciones preventivas y de mejora, documentar en el Plan de Mejoramiento Institucional y replantear los riesgos del proceso.
- Analizar y actualizar el mapa de riesgos.

18. 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.

19. 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.

20. 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.

21. 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 Sistema de Gestión de la Entidad sgc.dadep.gov.co y en la página Web de la entidad www.dadep.gov.co.

Elaboró: Iván Felipe Vargas Aldana - Contratista Oficina Asesora de Planeación
Revisó: Paula López Vendemiati, Jefe Oficina Asesora de Planeación.
Aprobó: Comité Institucional de Coordinación de Control Interno 24/12/2024
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). 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.

CONTROL DE CAMBIOS		
VERSIÓN	**FECHA**	**DESCRIPCIÓN DE MODIFICACIÓN**
		Se establecen tiempos y lineamientos en lo que corresponde a control, monitoreo y comunicación de las matrices de riesgos.