Alcaldía de Medellín
Distrito de
Ciencia, Tecnología e Innovación

SISTEMA INTEGRAL DE GESTIÓN - SIG

INFORME ADMINISTRACIÓN DE RIESGOS DE GESTIÓN

Primer Cuatrimestre 2025
Diciembre 01 2024 al 31 de marzo de 2025

Documento elaborado por:

Catalina Arenas Molina
Jhon Fredy Duque Castaño

Profesionales Universitarios

Secretaría de Gestión Humana y Servicio a la Ciudadanía
Subsecretaría de Desarrollo Institucional
Unidad de Planeación Organizacional

Medellín
Abril de 2025

TABLA DE CONTENIDO

LISTA DE ILUSTRACIONES

LISTA DE TABLAS

LISTA DE GRÁFICAS

INTRODUCCIÓN

El Distrito de Medellín comprometido con la mejora continua y dando cumplimiento a las disposiciones emitidas por el Departamento Administrativo de la Función y la Secretaría de la Presidencia de la República en la *"Guía para la administración del riesgo y el diseño de controles en entidades públicas-riesgos de gestión, corrupción y seguridad digital"* versión 5 de diciembre de 2020, con relación a la gestión de los riesgos de la entidad como un elemento preventivo, comparte con sus grupos de valor y grupos de interés el resultado de la autoevaluación realizada por los líderes responsables de los procesos en conjunto con sus equipos operativos como primera línea de defensa, en el periodo de diciembre 01 2024 al 31 de marzo de 2025.

Igualmente le corresponde a la Subsecretaría de Desarrollo Institucional como segunda línea de defensa, analizar y monitorear la autoevaluación y consolidar los datos en el presente Informe Administración de Riesgos de Gestión.

El informe evidencia el comportamiento de los *Riesgos de Gestión* establecidos para los veintisiete (27) procesos que conforman el Modelo de Operación de la Administración Distrital, nivel central y presenta las recomendaciones tendientes a cerrar las brechas en aquellos elementos que necesitan una mejora en su gestión.

1. FUNDAMENTO NORMATIVO

- *Guía para la Administración del Riesgo y el Diseño de Controles en las Entidades Públicas. Riesgos de Gestión, Corrupción y Seguridad Digital,* Versión 5 de diciembre de 2020.
- *Guía para la gestión por procesos en el marco del modelo integrado de planeación y gestión -MIPG,* versión 1 julio 2020.

2. OBJETIVO

Monitorear y revisar la gestión de riesgos de gestión ejecutada por la primera línea de defensa, complementando su trabajo y verificando que los controles estén diseñados apropiadamente y funcionen como se pretende.

3. ALCANCE

Comprende las actividades desarrolladas en la gestión de Riesgos de Gestión durante el primer cuatrimestre comprendido entre diciembre 01 2024 al 31 de marzo de 2025, acorde con lo establecido en el numeral *6.5 Periodicidad para el monitoreo y revisión de los riesgos*, del *MA-DIES-044 Manual Política Integral Administración de Riesgos*.

4. ASPECTOS GENERALES

4.1. Metodología

Para dar cumplimiento al objetivo propuesto, se utilizaron como elementos de análisis los lineamientos establecidos en la *Guía para la administración del riesgo y el diseño de controles en entidades públicas-riesgos de gestión, corrupción y seguridad digital*, versión 5 de diciembre de 2020, los *mapa y plan de tratamiento* de *riesgos y* actas *de autoevaluación de riesgos* documentados en la herramienta Isolución por los responsable de los veintisiete (27) procesos del Modelo de Operación del Distrito de Medellín.

4.2. Modelo de Operación

La unidad de análisis de los riesgos de gestión y corrupción, son los objetivos de los procesos que conforman el Modelo de Operación del Distrito de Medellín, establecido por el Decreto Distrital 0225 de 2022.

Ilustración 1. Modelo de Operación por Procesos

Vale la pena resaltar que con el Decreto 0225 de 2022 fue derogado el Decreto 1985 de 2015, y de acuerdo a este el Modelo de Operación por Procesos del Distrito de Medellín cuenta con un total de veintisiete (27) procesos, distribuidos en los niveles estratégico (1 proceso), misionales (15 procesos), de apoyo (10 procesos) y de evaluación y mejora (1 proceso).

5. ESTADO DE LOS RIESGOS DE GESTIÓN – PRIMER CUATRIMESTRE 2025

5.1 Universo riesgos (corrupción y gestión)

El universo de los riesgos lo constituyen los riegos de *gestión y corrupción* de los veintisiete (27) procesos que componen el Modelo de Operación por procesos, en los documentos denominados "*Mapa y Plan de Tratamiento de Riesgos".*

A corte 31 de marzo de 2025, la distribución de los riesgos de gestión y de corrupción, fue la siguiente:

Tipo Riesgo	Total Riesgos
Corrupción	68
Gestión	103
Total general	**171**

Gráfica 1 Tipo de riesgos VS Total de Riesgos

La gráfica 1 evidencia la identificación de ciento setenta y un (171) riesgos distribuidos en los veintisiete (27) procesos, de los cuales ciento tres (103) riesgos son de gestión y representan un sesenta por ciento (60%), y sesenta y ocho (68) riesgos son de corrupción que equivalen a un cuarenta por ciento (40%) del total de los riesgos.

5.2 Distribución Riesgos de Gestión por proceso

Los ciento tres un (103) riesgos de gestión identificados a corte 31 de marzo de 2025, se distribuyen en los veintisiete (27) procesos del Modelo de Operación, de la siguiente manera:

PROCESO	Total Riesgos
Direccionamiento Estratégico	9
Gestión de Hacienda Pública	9
Gestión del Desarrollo Económico	7
Gestión de la Salud	6
Gestión de la Tecnología de la Información y las Comunicacion	6
Evaluación y Mejora Institucional	5
Gestión de la Seguridad	5
Servicio a la Ciudadanía	5
Administración de Bienes Muebles e Inmuebles	4
Gestión Ambiental	4
Gestión del Riesgo de Desastres	4
Fortalecimiento de la Ciudadanía	3
Gestión Cultural	3
Gestión de la Educación	3
Gestión de la Información	3
Gestión de la Obra Pública	3
Gestión de Servicios Públicos Domiciliarios y No Domiciliarios	3
Gestión Integral del Talento Humano	3
Gestión Jurídica	3
Comunicación Pública	2
Gestión Catastral	2
Gestión de Compras Públicas Transparentes	2
Gestión de la Gobernanza Local	2
Gestión de la Movilidad	2
Gestión del Control Urbanístico	2
Gestión Social del Riesgo	2
Mantenimiento de Bienes Muebles e Inmuebles	1
Total general	103

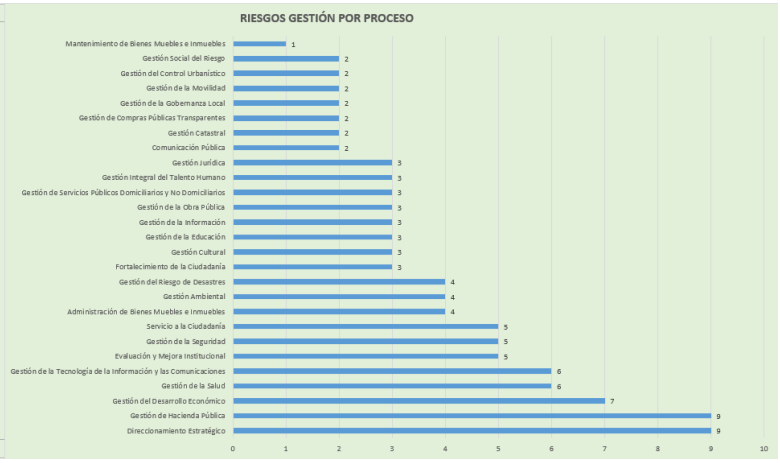


Tabla 1. Cantidad riesgos de gestión por proceso

Los procesos que cuentan con el mayor número de riesgos de gestión identificados son:

Proceso	Número de riesgos de gestión
Gestión de Hacienda Pública	9
Direccionamiento Estratégico	9
Gestión del Desarrollo Económico	7
Gestión de la Salud	6
Gestión de la Tecnología de la Información y las Comunicaciones	6
Evaluación y Mejora Institucional	5 (en cada proceso)
Gestión de la Seguridad	
Servicio a la Ciudadanía	
Administración de Bienes Muebles e Inmuebles	4 (en cada proceso)
Gestión Ambiental	
Gestión del Riesgo de Desastres	

Tabla 2. Procesos mayor cantidad de riesgos de gestión

De la información contenida en la tabla 2, se puede concluir que en once (11) procesos de la entidad se encuentra el sesenta y dos por ciento (62%) de los riesgos de gestión identificados.

5.3 Variación riesgos de gestión

Al comparar el número de riesgos de gestión identificados en los veintisiete procesos del Modelo de Operación del Distrito de Medellín formulados al principio de la vigencia 2025 con la autoevaluación del primer cuatrimestre del 2025, se evidencia hubo variación de

un riesgo de gestión en el Proceso de Gestión de la Seguridad; a principio de vigencia contaban con 4 riesgos y al corte de este informe incrementaron a 5.

Proceso	Cantidad de Riesgos de Gestión		
	Formulación 2025	1er Cuatrimestre 2025	Variación
Administración de Bienes Muebles e Inmuebles	4	4	0
Comunicación Pública	2	2	0
Direccionamiento Estratégico	9	9	0
Evaluación y Mejora Institucional	5	5	0
Fortalecimiento de la Ciudadanía	3	3	0
Gestión Ambiental	4	4	0
Gestión Catastral	2	2	0
Gestión Cultural	3	3	0
Gestión de Compras Públicas Transparentes	2	2	0
Gestión de Hacienda Pública	9	9	0
Gestión de la Educación	3	3	0
Gestión de la Gobernanza Local	2	2	0
Gestión de la Información	3	3	0
Gestión de la Movilidad	2	2	0
Gestión de la Obra Pública	3	3	0
Gestión de la Salud	6	6	0
Gestión de la Seguridad	4	5	1
Gestión de la Tecnología de la Información y las Comunicaciones	6	6	0
Gestión de Servicios Públicos Domiciliarios y No Domiciliarios	3	3	0
Gestión del Control Urbanístico	2	2	0
Gestión del Desarrollo Económico	7	7	0
Gestión del Riesgo de Desastres	4	4	0
Gestión Integral del Talento Humano	3	3	0
Gestión Jurídica	3	3	0
Gestión Social del Riesgo	2	2	0
Mantenimiento de Bienes Muebles e Inmuebles	1	1	0
Servicio a la Ciudadanía	5	5	0
Total Riesgos por Cuatrimestre	**102**	**103**	**1**
Variación Porcentual		**1%**	

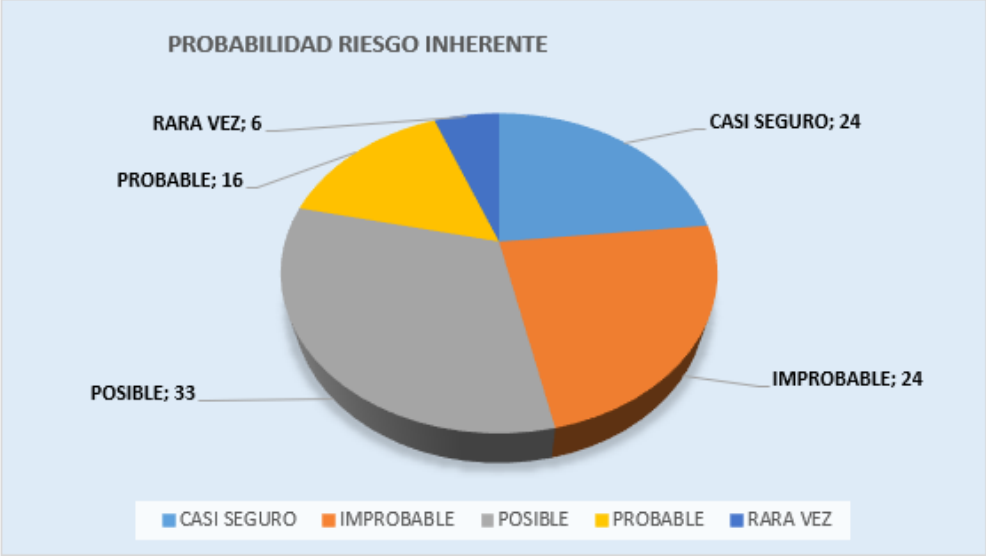
Fuente: Mapas y Plan de tratamiento de riesgos de gestión
Tabla 3. Variación riesgos de gestión

El nuevo riesgo que se incluyó en el proceso de Gestión de la Seguridad fue: "Posibilidad de afectación económica y reputacional por emitir respuestas a las solicitudes de PQRSD que interponen los ciudadanos incumpliendo los requisitos de calidad y los atributos establecidos en la normatividad vigente debido a elaboración y/o entrega de la respuesta de las solicitudes de la ciudadanía (PQRSD) sin el lleno de los atributos de calidad contemplados, los cuales son; respuestas de fondo, claras, congruentes, oportunas y con una notificación eficaz".

5.4 Probabilidad de ocurrencia

La probabilidad de ocurrencia de los *riesgos de gestión*, se califica bajo criterios de frecuencia "rara vez", "improbable", "posible", "probable" y "casi seguro". En la gráfica 2 se presenta la probabilidad de ocurrencia inherente de los *riesgos de gestión*:

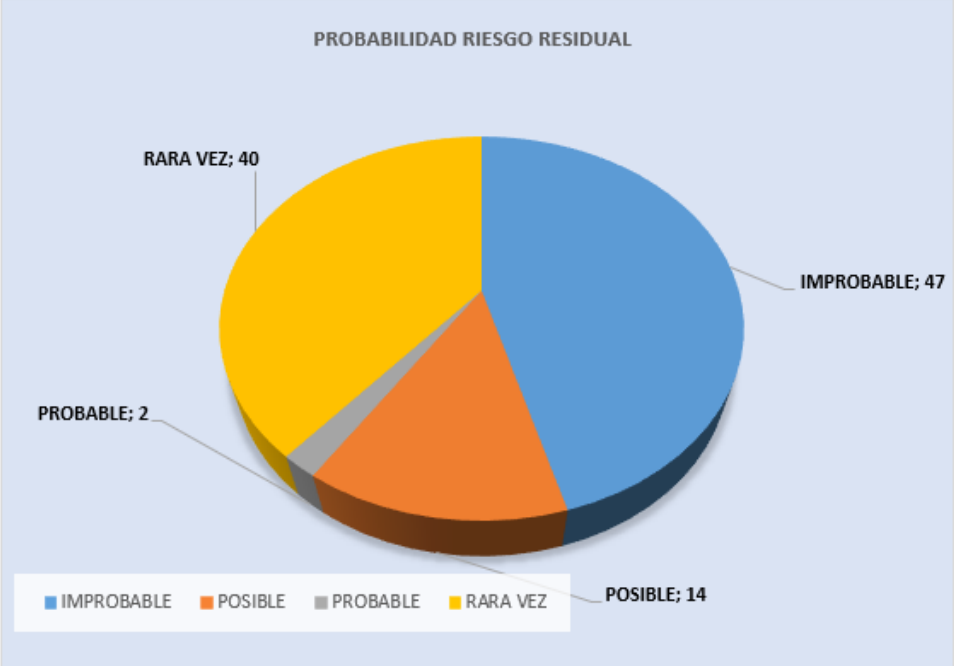
PROBABILIDAD RIESGO INHERENTE	Total
CASI SEGURO	24
IMPROBABLE	24
POSIBLE	33
PROBABLE	16
RARA VEZ	6
Total general	**103**



Gráfica 2 Probabilidad de ocurrencia riesgos inherentes

Una vez se diseñen y ejecuten los controles, la probabilidad de ocurrencia de los riesgos debe cambiar de zona, tal y como se evidencia en la gráfica 3.

PROBABILIDAD RIESGO RESIDUAL	Total
IMPROBABLE	47
POSIBLE	14
PROBABLE	2
RARA VEZ	40
Total general	**103**



Gráfica 3 Probabilidad ocurrencia riesgo residual

5.5 Naturaleza del control en los riesgos de gestión

Los controles tienen como finalidad modificar el riesgo, la gráfica 4 muestra que para los ciento tres (103) *riesgos de gestión* definidos en la entidad, se diseñaron un total de doscientos cuarenta (240) controles, que se clasifican en controles preventivos (55 %), detectivos (39%) y correctivos (6%).

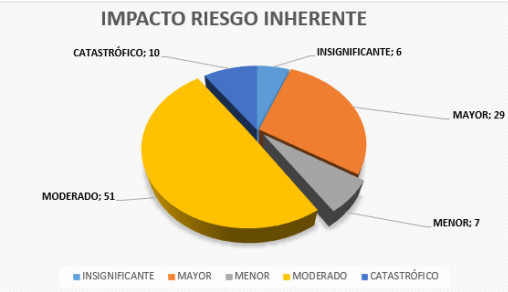
NATURALEZA DEL CONTROL RIESGOS GESTIÓN	
DESCRIPCIÓN DEL CONTROL	Total Controles
Detectivo	94
Preventivo	133
Correctivo	13
Total general	**240**

Gráfica 4 Descripción del Control vs Total Controles

5.6 Zona de impacto riesgo inherente y residual

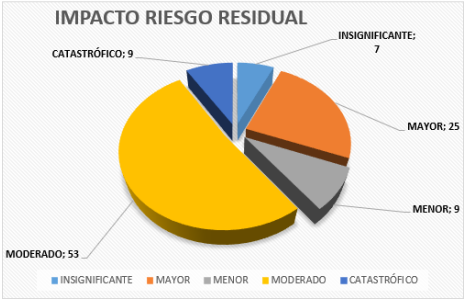
Acorde con lo establecido en la metodología utilizada por parte del Distrito de Medellín para la administración del riesgo, a los riesgos de gestión les aplica los niveles de impacto "Insignificante", "Menor", "Moderado", "Mayor" y "Catastrófico. Así mismo se establece que con la ejecución de controles se puede presentar disminución de probabilidad e/o impacto. En las gráficas 5 y 6, se evidencia la clasificación de zona de impacto de los riesgos "inherente" y "residual".

IMPACTO RIESGO INHERENTE POR ZONA	Total Riesgos
INSIGNIFICANTE	6
MAYOR	29
MENOR	7
MODERADO	51
CATASTRÓFICO	10
Total general	**103**



Gráfica 5 Zona inherente riesgo de gestión

IMPACTO RIESGO RESIDUAL POR ZONA	Total Riesgos
INSIGNIFICANTE	7
MAYOR	25
MENOR	9
MODERADO	53
CATASTRÓFICO	9
Total general	**103**



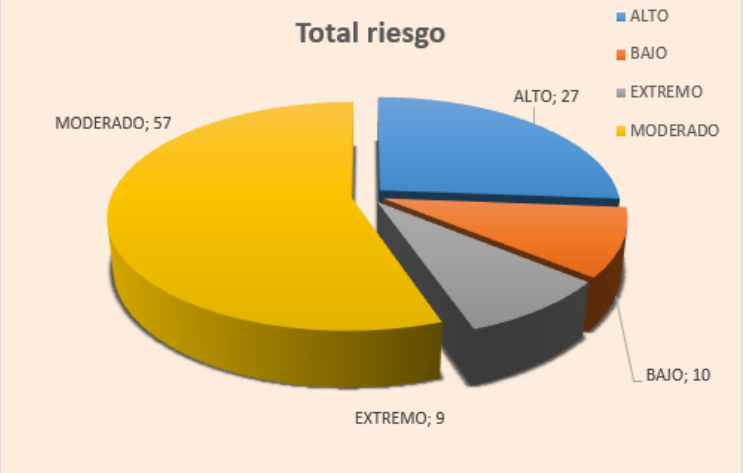
Gráfica 6 Zona residual riesgos de gestión

Al analizar las gráficas relacionadas con las zonas de impacto de los riesgos de gestión de la entidad, se evidencia desplazamiento en el Impacto en 10 riesgos; esto porque la mayoría de controles definidos por la entidad son de tipo preventivo y detectivo, afectando solo la probabilidad.

5.7 Zona de riesgo residual

Una vez realizado el análisis y evaluación de los controles para la mitigación de los riesgos, se establece el nivel del riesgo residual, clasificándolo por zonas de riesgo, tal y como se evidencia en la gráfica 7.

RIESGOS RESIDUAL POR ZONA	
ZONA DE RIESGO	Total riesgo
ALTO	27
BAJO	10
EXTREMO	9
MODERADO	57
Total general	**103**



Gráfica 7 Zona de riesgo residual

Del total de los *riesgos de gestión* definidos en el Distrito de Medellín, los riesgos ubicados en zona extrema (9); alto (27) y moderado (57) que equivalen al 90%, deben contar con controles que permitan REDUCIR la probabilidad de ocurrencia del riesgo.

5.8 Riesgos de gestión materializados

Para el primer cuatrimestre de 2025, los líderes de los procesos realizaron la autoevaluación de los *riesgos de gestión*, teniendo en cuenta entre otros los siguientes insumos:

- DE-DIES-167 Contexto Interno y Externo, versión 6
- Guía para la administración de riesgos y el diseño de controles en entidades públicas, versión 5
- DE-DIES-036 Política Integral de Administración de Riesgos Distrito de Medellín, versión 5
- MA-DIES-044 Manual Política Integral Administración de Riesgos, versión 9
- Reporte Sanciones Proferidas, remitido por la Unidad Administración de Personal
- Informe de PQRSD. Periodo noviembre 2024 a febrero 2025, remitido por la subsecretaria de Servicio a la Ciudadanía.

- Relación de fallos sancionatorios disciplinarios, remitido por parte del Equipo de Control Disciplinario Interno.
- Informes de las evaluaciones independientes realizadas, auditorias ejecutadas por parte de la secretaria de Evaluación y Control.

La evidencia de la autoevaluación de los *riesgos de gestión* por parte de los líderes de los procesos en conjunto con sus equipos, reposa en "Actas" y documentos específicos "*DE Mapa y plan de tratamiento de riesgos*", documentados en la herramienta Isolución para cada uno de los veintisiete (27) procesos.

De los ciento tres (103) riesgos de gestión identificados en los veintisiete (27) procesos, durante el primer cuatrimestre se evidencia la materialización de catorce (14) riesgos, como lo muestra la gráfica 8.

RIESGOS MATERIALIZADOS	
Materializó	**Total**
No	89
Si	14
Total general	**103**

Gráfica 8 Materialización riesgos de gestión

Los *riesgos de gestión* materializados (14), se distribuyeron en trece (13) de los veintisiete (27) procesos, tal y como se presenta en la gráfica 9; igualmente se evidencia que los procesos con mayor número de *riesgos de gestión* materializados es Gestión Catastral con 2 riesgos, los 12 procesos restantes materializaron de a un riesgo de gestión.

RIESGOS MATERIALIZADOS	
PROCESO	Total
Direccionamiento Estratégico	1
Fortalecimiento de la Ciudadanía	1
Gestión Ambiental	1
Gestión Catastral	2
Gestión de Compras Públicas Transparentes	1
Gestión de la Gobernanza Local	1
Gestión de la Movilidad	1
Gestión de la Obra Pública	1
Gestión de la Salud	1
Gestión de la Seguridad	1
Gestión de la Tecnología de la Información y las Comunicaciones	1
Gestión del Control Urbanístico	1
Gestión del Riesgo de Desastres	1
Total general	14

Gráfica 9 Riesgos materializados por proceso

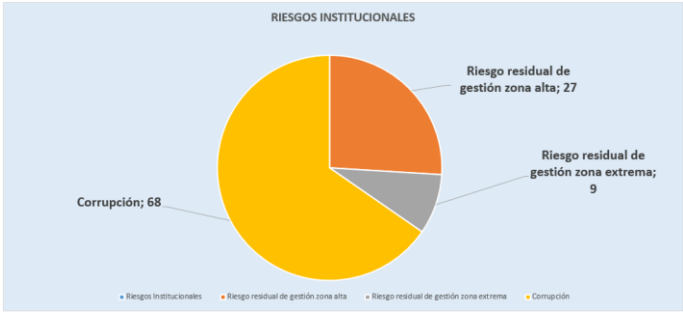
En el anexo 1 *Descripción Riesgos Materializados Por Proceso,* se encuentran los riesgos materializados, clasificados por proceso, el acta que evidencia la autoevaluación, la acción de mejora formulada por parte de los directivos que lideran procesos en conjunto con sus equipos, con el fin de mitigar las causas que originaron la materialización del riesgo, y observaciones relevantes en cada caso.

6. RIESGOS INSTITUCIONALES

6.1 Riesgos Institucionales

Los *Riesgos Institucionales* contienen a nivel estratégico todos *los riesgos de gestión residuales* ubicados en zona "Alta" y "Extrema" y los "*riesgos de corrupción"* de cada uno de los procesos que pueden afectar el cumplimiento de la misión y metas institucionales; evidenciado en la gráfica 10.

Riesgos Institucionales	
Riesgo residual de gestión zona alta	27
Riesgo residual de gestión zona extrema	9
Corrupción	68
Total general	104



Gráfica 10 Riesgos Institucionales

En la tabla 4 (riesgos de gestión en zona alta, 27 riesgos) y tabla 5 (riesgos de gestión en zona extrema, 9 riesgos), se relacionan la distribución de riesgos por proceso, lo que

permite identificar los procesos en la entidad más vulnerables en caso de materializarse un riesgo de gestión.

ZONA RIESGO RESIDUAL ALTA POR PROCESOS	
PROCESO	TOTAL RIESGOS
Administración de Bienes Muebles e Inmuebles	2
Direccionamiento Estratégico	4
Gestión Ambiental	1
Gestión de Hacienda Pública	6
Gestión de la Educación	1
Gestión de la Movilidad	1
Gestión de la Seguridad	1
Gestión de la Tecnología de la Información y las Comunicaciones	1
Gestión del Desarrollo Económico	7
Gestión del Riesgo de Desastres	1
Gestión Social del Riesgo	2
Total general	27

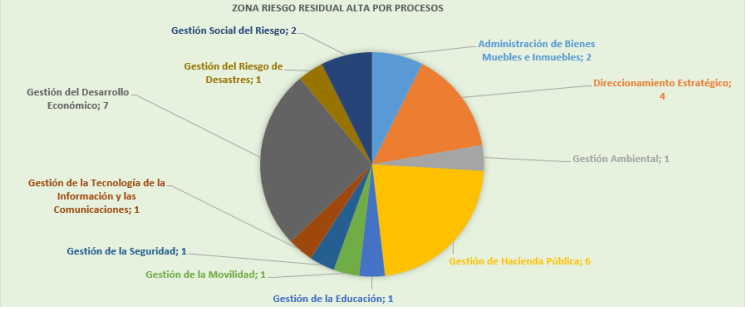


Tabla 4. Zona de riesgo residual alta

ZONA RIESGO RESIDUAL EXTREMA POR PROCESOS	
PROCESO	TOTAL RIESGOS
Administración de Bienes Muebles e Inmuebles	1
Direccionamiento Estratégico	1
Gestión de Compras Públicas Transparentes	2
Gestión de la Educación	2
Gestión de la Salud	2
Gestión de la Tecnología de la Información y las Comunicaciones	1
Total general	9

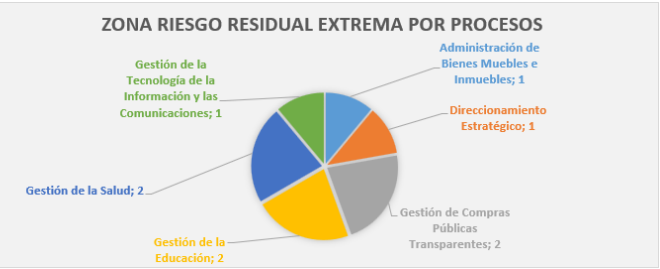


Tabla 5. Zona de riesgo residual extrema

Se puede concluir que los riesgos de gestión residuales ubicados en zona “Alta” y “Extrema” representan el treinta y cinco por ciento (35%) de los *Riesgos Institucionales* del Distrito de Medellín.

7. SEGUIMIENTO RIESGOS SEGURIDAD INFORMÁTICA

La gestión basada en riesgos se convierte en el pilar fundamental para la prevención, mitigación de situaciones que puedan generar un impacto significativo al cumplimiento de las metas organizacionales, bien sea incidiendo directa o indirectamente, afectando la cadena de procesos organizacional y generando con ello afectaciones a la prestación de servicios o incluso llegando al incumplimiento de los objetivos organizacionales.

La identificación, valoración y seguimiento de riesgos de seguridad informática como aporte a la hoy denominada seguridad digital, en términos de la guía para la implementación de riesgos y el diseño de controles publicada por el Departamento Administrativo de la Función Pública y articulada al fortalecimiento de las entidades públicas con las propuestas emanadas desde el Ministerio de Tecnologías de Información y de las Comunicaciones a través de la Política de Gobierno Digital, se convierten en un insumo de valor para la toma de decisiones organizacionales, de tal manera que oriente

la inversión y el fortalecimiento administrativo para apalancar los procesos que demanda una adecuada gestión del riesgo, así como la implementación de controles necesarios.

En ese contexto, surge este seguimiento a la materialización de riesgos frente a ciberamenazas que se identifican, analizan y valoran desde la unidad de seguridad informática y que en esta presentación corresponden al seguimiento entre los meses de diciembre 2024 a marzo de la vigencia 2025.

Contexto de los Riesgos Frente a Ciberamenazas

Para poder comprender el seguimiento realizado en el último cuatrimestre a los riesgos frente a ciberamenazas identificados y valorados desde la Unidad de Seguridad Informática, se precisa el listado de riesgos que definen el enfoque y alcance del seguimiento realizado en el periodo de reporte:

No.	Riesgo de seguridad informática
1	Afectación de la disponibilidad, integridad o confidencialidad de los **servidores**, por acción de operadores de **botnets**, debido a una falta o deficiencia en controles sobre la detección, prevención, recuperación para proteger contra códigos maliciosos.
2	Afectación de la disponibilidad, integridad o confidencialidad de los **servidores**, por acción de **Spyware/Malware**, debido a una falta o deficiencia en controles sobre la detección, prevención, recuperación para proteger contra códigos maliciosos.
3	Compromiso de la disponibilidad, integridad o confidencialidad de los **endpoints fijos, endpoints portátiles o endpoints estaciones ingeniería**, por acción de operadores **botnets**, debido a una falta o deficiencia en controles sobre la detección, prevención, recuperación para proteger contra códigos maliciosos
4	Compromiso de la disponibilidad, integridad o confidencialidad de **los endpoints fijos, endpoints portátiles o endpoints estaciones ingeniería**, por acción de **Spyware/Malware**, debido a una falta o deficiencia en controles sobre la detección, prevención, recuperación para proteger contra códigos maliciosos
5	Compromiso de la disponibilidad, integridad o confidencialidad de **los endpoints fijos, endpoints portátiles o endpoints estaciones ingeniería**, por acción de **Spyware/Malware**, debido a una falta o deficiencia en controles para los **medios removibles**
6	Afectación de la disponibilidad, integridad o confidencialidad de los **servidores**, por acción **hackers**, debido a una falta o deficiencia en controles de seguridad informática en la **gestión de las redes**

7	Afectación de la disponibilidad, integridad o confidencialidad de los **servidores**, por acción **hackers**, debido a una falta o deficiencia en controles sobre el **acceso a redes y servicios en red**
8	Afectación de la disponibilidad, integridad o confidencialidad de los servidores, por acción hackers, debido a una falta o deficiencia en controles que garanticen el procedimiento de ingreso seguro de inicio de sesión
9	Afectación de la disponibilidad, integridad o confidencialidad de los sistemas de información web, por acción de hackers, debido a una falta o deficiencia en controles que garanticen el adecuado análisis y especificación de requisitos de seguridad informática en los sistemas de información
10	Afectación de la disponibilidad, integridad o confidencialidad de los sistemas de información web, por acción de atacantes internos, debido a una falta o deficiencia en controles que garanticen el adecuado análisis y especificación de requisitos de seguridad informática en los sistemas de información
11	Afectación de la confidencialidad de los sistemas de información web, por acción de CiberDelincuentes, debido a una falta o deficiencia en controles que garanticen el adecuado análisis y especificación de requisitos de seguridad informática en los sistemas de información
12	Afectación de la disponibilidad, integridad o confidencialidad de los sistemas de información web, por acción de hackers, debido a una falta o deficiencia en el establecimiento y cumplimiento de una política sobre el uso de controles criptográficos
13	Afectación de la disponibilidad, integridad o confidencialidad de los servidores, por acción de hackers, debido a una falta o deficiencia en controles que garanticen la adecuada gestión de las vulnerabilidades técnicas
14	Afectación de la disponibilidad, integridad o confidencialidad de los servidores, por acción de atacantes internos, debido a una falta o deficiencia en controles que garanticen la adecuada gestión de las vulnerabilidades técnicas
15	Afectación de la disponibilidad de los accesos a internet dedicados, por acción de hackers, debido a una falta o deficiencia en el mantenimiento y control de las redes, que dificulta la protección contra las amenazas y la gestión de seguridad de los sistemas y aplicaciones que usan la red
16	Afectación de la integridad de los motores de bases de datos, por acción de atacantes internos, debido a una falta o deficiencia en controles que garanticen el adecuado registro de eventos y actividad en los activos informáticos

17	Afectación de la integridad, disponibilidad y confidencialidad del servicio de correo electrónico institucional, por acción de un ataque de phishing, debido a una falta o deficiencia en la toma de conciencia, educación y formación en la seguridad informática

Tabla 6. Agrupación de los Riesgos de Seguridad Informática

8. Seguimiento a los Riesgos de seguridad informática identificados y sus materializaciones.

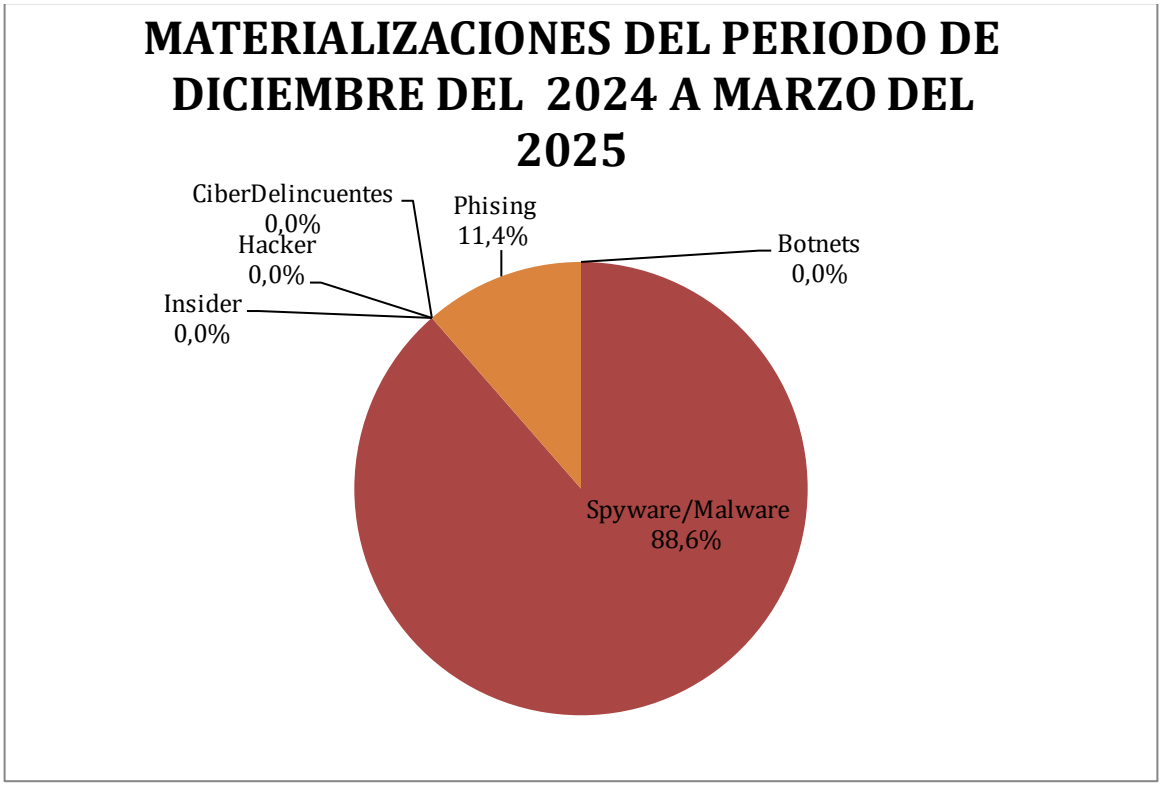
En concordancia con los riesgos previamente identificados y valorados, se presenta a continuación el detalle de las materializaciones ocurridas durante el periodo de análisis, estructuradas en la siguiente tabla. Esta información permite evidenciar el impacto real de las amenazas sobre los activos tecnológicos de la entidad y orientar la toma de decisiones frente a la gestión de seguridad informática:

POSIBLE AFECTACIÓN DE LA DISPONIBILIDAD / INTEGRIDAD / CONFIDENCIALIDAD DEL ACTIVO DE TECNOLOGÍA DE INFORMACIÓN (DICIEMBRE 2024 – MARZO 2025)		
No.	Activo de T.I. - Amenaza	Materializaciones
1	Servidores - Botnets	0
2	Servidores - Spyware/Malware	0
3	EndPoints - Botnets	0
4	EndPoints - Spyware/Malware	30
5	Medios Removibles de EndPoints - Spyware/Malware	1
6	Gestion de Redes - Hacker	0
7	Acceso a Redes - Hacker	0
8	Inicio de Sesión en Servidores - Hacker	0
9	Sistemas de Información Web - Hacker	0
10	Sistemas de Información Web - Insider	0
11	Sistemas de Información Web - Ciberdelincuentes	0
12	Criptografía sobre Sistemas de Información Web - Hacker	0
13	Vulnerabilidades en Servidores - Hacker	0
14	Vulnerabilidades en Servidores - Atacantes Interno	0
15	Disponibilidad de accesos - Hacker	0
16	Bases de Datos - Atacantes Internos	0
17	Correo Electrónico Institucional - Phishing	4
	TOTAL DE MATERIALIZACIONES	35

Tabla 7. Afectación de la Disponibilidad

El total de materializaciones en el periodo fue de 35 en relación con los grupos de riesgos identificados, de los cuales el 88,6% están relacionados con Spyware/Malware que ha

afectado equipos de usuario final y el 11.4 % está relacionado con phishing en correo Electrónico Institucional. Tal como se puede apreciar en la siguiente gráfica:

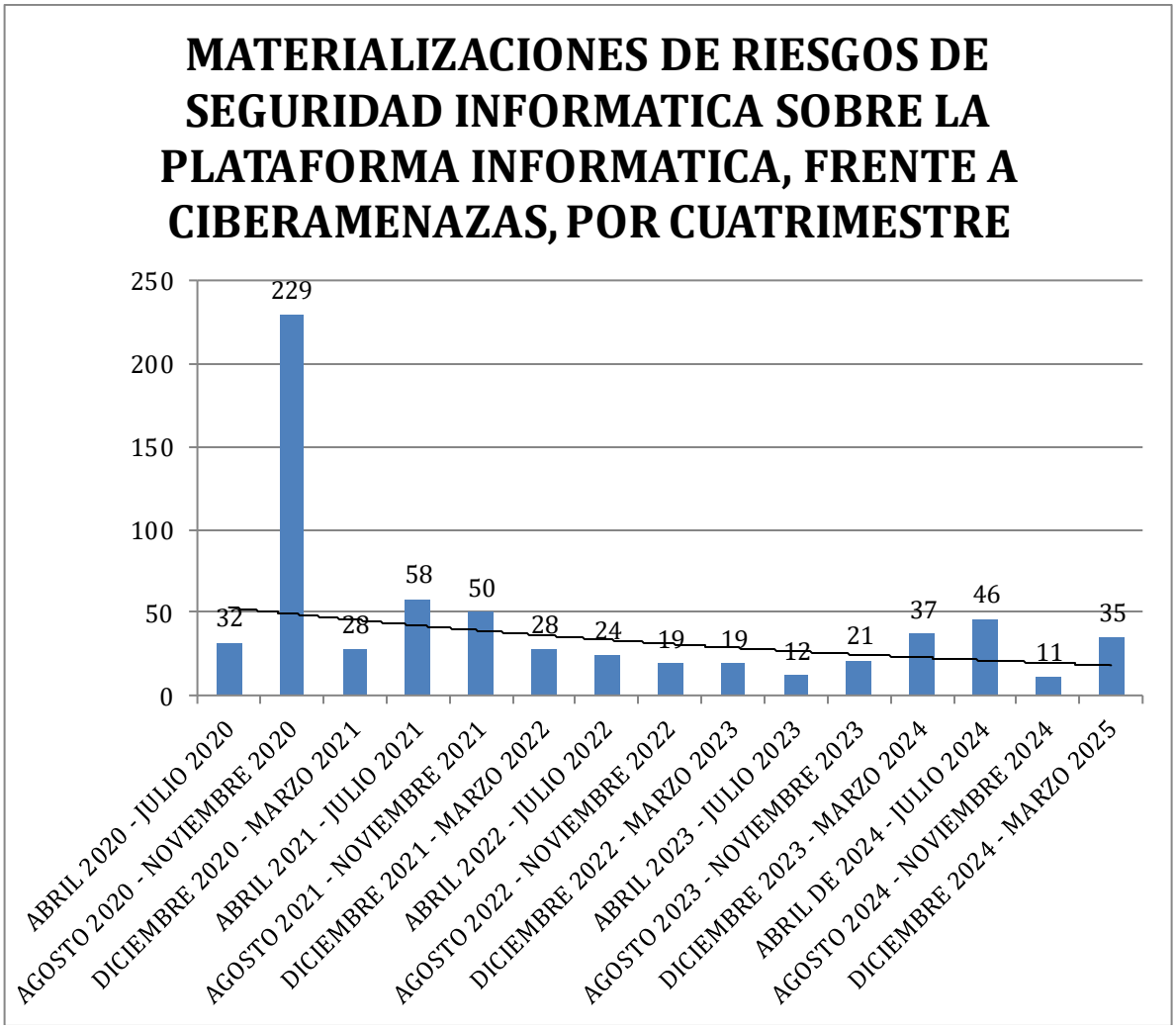


Gráfica 11 Materializaciones del periodo

ANALISIS POR FUENTE DE AMENAZAS EN EL PERIODO DICIEMBRE 2024 – MARZO 2025	
Amenazas	Materializaciones
Botnets	0
Spyware/Malware	31
Hacker	0
Insider	0
CiberDelincuentes	0
Phishing	4
TOTAL	35

Tabla 8. Análisis por fuente de amenazas en el periodo

Se puede observar referente a las materializaciones que se evidencia un aumento del 218,2% en comparación con las materializaciones del cuatrimestre anterior, tal como se presenta en la siguiente gráfica:



Gráfica 12 Clasificación Materializaciones del periodo

Este comportamiento refleja transformaciones en el panorama global de amenazas que enfrenta la organización, donde las materializaciones están directamente relacionadas con dichas variaciones. La dinámica cambiante de los ataques ha impactado diversos activos tecnológicos, lo que evidencia la necesidad de fortalecer continuamente los mecanismos de defensa y resiliencia digital. En particular, la presencia de malware en estaciones de trabajo y otros componentes de infraestructura tecnológica exige la

implementación de acciones proactivas y sostenidas para preservar la confidencialidad, integridad y disponibilidad de los datos institucionales.

A continuación, se presenta la gráfica correspondiente a la distribución de las materializaciones, segmentadas por tipo de activo y amenaza. Durante el cuatrimestre analizado, se observa que el 85,7% de los casos correspondieron a malware en estaciones de usuario final, seguido de un 2,9% por infección a través de medios removibles. Así mismo, se identificaron materializaciones de phishing en el correo electrónico institucional que representaron un 11,4% del total de incidentes registrados:

Gráfica 13 Materializaciones en el periodo

Es prioritario destacar que las materializaciones registradas en estaciones de usuario final reflejan no solo un riesgo técnico, sino una necesidad urgente de fortalecer las capacidades humanas para la seguridad informática de la organización. Estos incidentes, en muchos casos, están relacionados con prácticas inadecuadas en el uso de los recursos informáticos por parte de servidores públicos y contratistas, lo que evidencia la

importancia de avanzar hacia una cultura institucional de corresponsabilidad en la seguridad informática institucional.

9. CONCLUSIONES

- La gestión del riesgo en el Distrito de Medellín se encuentra alineada con el Modelo Integrado de Planeación y Gestión – MIPG a través de cuatro dimensiones, fundamentalmente en lo referente a los riesgos asociados a los procesos que conforman el Sistema Integral de Gestión (SIG) de la Entidad.

- Se integra a la gestión formal del riesgo que se lleva a cabo en la Entidad aquellos riesgos que están siendo gestionados siguiendo los lineamientos definidos por las respectivas entidades rectoras del orden nacional. Tales riesgos son los asociados a: proyectos de inversión, contratación, seguridad y salud en el trabajo y seguridad de la información (seguridad digital).

- Las materializaciones siguen evidenciando la potencialidad de las amenazas reconocidas como Malware o Código Malicioso que pueden colocar en riesgo la disponibilidad de la información corporativa, siendo necesario incrementar los esfuerzos no solo en materia de seguimiento, detección y remediación, sino de fortalecer los procesos de sensibilización y concienciación de los usuarios finales.

- La unidad de seguridad informática continúa dedicando sus esfuerzos en contener y generar acciones para erradicar este tipo de malware, sin embargo, requiere de un proceso de detección y respuesta constante, por lo cual, se continuará realizando las siguientes actividades:

  - ✓ Con la implementación de la solución antimalware se ha fortalecido la visibilidad, en términos de eventos o incidentes que pueden afectar la plataforma informática, a partir de la cual se han podido emprender acciones más efectivas para la remediación en articulación con equipos responsables del soporte a la infraestructura tecnológica de la organización.

  - ✓ Se cuenta con una planeación para adelantar jornadas de sensibilización para todos los servidores públicos y contratistas de la entidad, en el que se abordaran temas de formación en el uso adecuado de los servicios y recursos informáticos de la Entidad, como estrategia para mitigar las materializaciones que se vienen presentando en la entidad por malware y phishing, esperando que la participación de los servidores públicos y contratistas sea alta.

- El incremento en los métodos y capacidades de ataque por parte de cibercriminales a las organizaciones ha venido afectando a diferentes entidades públicas y privadas en el ámbito nacional e internacional, que incrementan la probabilidad de materialización de los riesgos frente a ciberamenazas en la entidad, por lo cual se requiere de apoyo de la alta dirección para:

  - ✓ Destinar recursos para fortalecer medidas de seguridad requeridas en atención a la infraestructura tecnológica del Distrito y coherentes con lo expuesto en la resolución 0500 de 2021, en relación con la adquisición de controles de seguridad tales como: La protección perimetral de acceso a bases de datos institucionales, la solución correlacionadora de eventos de seguridad informática para apalancar lo dispuesto en el artículo 17 de la resolución 0500 de 2021, entre otros servicios identificados.

- La totalidad de procesos de la entidad, realizaron monitoreo y revisión a los riesgos de gestión, detectando acciones para abordar riesgos que permitan el cierre de brechas en la materialización de riesgos de gestión.

- Se cumplió con la publicación oportuna del mapa de riesgos de gestión del primer cuatrimestre de 2025, en la página web institucional, link de Transparencia / 4.3 Plan de acción/ Planes Institucionales y Estratégicos (Decreto 612 de 2018)/ Plan Anticorrupción y de Atención al Ciudadano.

- La Unidad de Planeación Organizacional como segunda línea de defensa, realizó la verificación al cumplimiento de la autoevaluación de los riesgos de gestión de la primera línea de defensa (líderes de los procesos), a través del documento *FO-EVMI Monitoreo y revisión de los riesgos y actividades de control*, el cual quedó como registro en el acta de riesgos de cada proceso.

- El Distrito de Medellín cuenta con doscientos cuarenta (240) controles para los riesgos de gestión, los cuales cumplen con los 6 criterios de control y se expresan de manera completa en el documento "*mapa y plan de tratamiento de riesgos*" de cada proceso.

- De los ciento tres (103) riesgos de gestión identificados en los veintisiete (27) procesos, se evidencia la materialización de 14 riesgos, correspondiente al 13% del universo de riesgos de gestión de la entidad.

- Para el primer cuatrimestre del año 2025 hubo cambios en el número de riesgos de gestión de la entidad con respecto a los formulados en el principio de vigencia 2025; se incluyo un nuevo riesgo en el proceso de Gestión de la Seguridad.

10. RECOMENDACIONES

- Fortalecer el proceso de consolidación de evidencias de la ejecución y efectividad de los controles definidos para las causas de los riesgos de gestión, por parte de los líderes de proceso y sus equipos de trabajo.

- Los directivos que lideran procesos en conjunto con sus equipos, deben realizar seguimiento y monitoreo a las acciones de mejora que se identificaron para los riesgos materializados, a través del software ISOLUCIÓN.

- Dar continuidad a la gestión de riesgos de seguridad informática, para lo cual se requiere la gestión de la Subsecretaría de Servicios de Tecnología de la Información en corresponsabilidad con todos los líderes de los procesos.

ANEXO 1

DESCRIPCIÓN RIESGOS MATERIALIZADOS POR PROCESO					
PRIMER CUATRIMESTRE 2025 Trece (14) riesgos materializados					
N°	**Proceso**	**Acta**	**Riesgo Materializado**	**Acción de Mejora**	**Observación**
1	Direccionamiento Estratégico	Dep-DIES - 58	Posibilidad de afectación reputacional por Inoportunidad en la gestión de las PQRSD de Direccionamiento Estratégico debido a Asignación inadecuada como PQRSD de los trámites del ordenamiento territorial, Asignación inadecuada de PQRSD y trámites a servidores o equipos de trabajo del proceso DIES.	5269	El riesgo se materializó debido a que no se cumplió con el indicador de oportunidad en la respuesta de las PQRSD. Las causas de materialización del riesgo que se identificaron son: *Dificultades en el Sistema de Información Documental Mercurio, debido al cambio de versión. *Para el caso de las PQRSD responsabilidad de la Unidad de Atención y Aplicación de la Norma Urbanística, se identificó sobrecarga laboral e insuficiente recurso humano para responder a la demanda de solicitudes que ingresaron en el periodo autoevaluado y fallas en el visor Mapgis que dificulta la consulta de la información requerida para dar respuesta.
2	Fortalecimiento de la Ciudadanía	SECRETARIA DE PARTIC-FOCI - 99	Posibilidad de afectación económica y reputacional por Falta de direccionamiento para la generación, recolección, almacenamiento y disposición de la información al interior de la dependencia. debido a falta de información de beneficiarios directos e indirectos, Desconocimiento y falta de aplicación de los sistemas de información existentes	2758	El análisis de las evidencias de los controles implementados, permitió llegar a la conclusión de la materialización del riesgo para el período de la autoevaluación. Es imperativo implementar medidas inmediatas para garantizar el cumplimiento de los objetivos de planificación de bienes, servicios y procesos, debido a desviaciones producidas por el equipo de trabajo durante el período de autoevaluación. Además, se ha presentado un incidente externo con la sentencia No. 215 del Tribunal Administrativo de Antioquia - Sala Quinta de Decisión, que revoca y declara nulidad parcial de ciertos artículos relacionados con el Sistema Municipal de Planeación del Municipio de Medellín. Por lo tanto, es necesario tomar medidas correctivas para subsanar estas deficiencias.

DESCRIPCIÓN RIESGOS MATERIALIZADOS POR PROCESO					
PRIMER CUATRIMESTRE 2025 Trece (14) riesgos materializados					
N°	**Proceso**	**Acta**	**Riesgo Materializado**	**Acción de Mejora**	**Observación**
3	Gestión Ambiental	SECRETARIA DE PARTIC-FOCI - 99	Posibilidad de afectación económica y reputacional por inoportunidad en las intervenciones ambientales planeadas en todas las zonas y corregimientos del Distrito Especial de Ciencia, Tecnología e Innovación de Medellín, debido a la baja disponibilidad de recursos financieros, insuficiente disponibilidad de personal idóneo, restricciones generadas por políticas públicas, deficiencia en la interacción con otros procesos, deficiencia en la interacción entre Unidades y Equipos de Trabajo al interior de la Secretaría de Medio Ambiente	2760	"A causa de la baja disponibilidad de recursos financieros.
4	Gestión Catastral	Sub-GCAT - 37	Posibilidad de afectación económica y reputacional por Incumplimiento en los tiempos respuesta a las solicitudes catastrales presentadas por los contribuyentes debido a Asignación inoportuna e insuficiente de recursos humanos y económicos requeridos para atender la demanda de solicitudes, Falta de Autocontrol, Incumplimiento en la ejecución contractual por parte del tercero de apoyo a la gestión catastral, Represamiento de tramites,	2722	"Se presentó incumplimiento en la oportunidad de respuesta del 39% de los 4,823 trámites ingresados en el periodo de 01 de diciembre de 2024 al 31 de marzo
5	Gestión Catastral	Sub-GCAT - 37	Posibilidad de afectación económica y reputacional por Intermitencia y dificultades, tanto en la conectividad, en el acceso y en el cambio de versión de las diferentes plataformas tecnológicas del distrito de Medellín y que utiliza la Subsecretaría de Catastro, para realizar su	5360	No se ha logrado obtener la efectividad necesaria para el adecuado funcionamiento de las plataformas, por parte de la Subsecretaria de Innovación Tecnológica

DESCRIPCIÓN RIESGOS MATERIALIZADOS POR PROCESO					
PRIMER CUATRIMESTRE 2025 Trece (14) riesgos materializados					
N°	**Proceso**	**Acta**	**Riesgo Materializado**	**Acción de Mejora**	**Observación**
			gestión catastral debido a ausencia de planeación y controles adecuados por parte de la Secretaría de Innovación Digital, para prestar los servicios de manera eficaz y eficiente , cambios en la versión del software que afecta la operación catastral y hardware obsoletos o deficientes, , ,		
6	Gestión de Compras Públicas Transparentes	Sec-GECO-36	Posibilidad de realizar una acción errónea o equivocada en una o varias tareas de uno de los procedimientos del proceso de Gestión de Compras Públicas Transparentes	2759 y 2736	"La materialización de este riesgo se dio porque en el periodo comprendido entre el 16 de noviembre de 2024 y el 15 de marzo de 2025, la Secretaría de Gestión y Control Territorial informó que fueron remitidos los documentos necesarios para la compra de las sillas, "Suministro de muebles y enseres", en la fecha indicada, pero hasta el momento aún no han sido adquiridas por parte de la Secretaría de Suministros y Servicios.
7	Gestión de la Gobernanza Local	Sec-GGOL-47	Posibilidad de afectación reputacional por Inoportunidad para dar respuesta según los términos de Ley y en el desarrollo de los procesos asociados, a las PQRSD, trámites y demás solicitudes, debido a Alta cantidad de PQRSD, trámites y demás solicitudes, con poca capacidad de respuesta de las dependencias que participan en el proceso, aumento en la cantidad de solicitudes virtuales que ingresan como PQRSD, por influencia de factores exógenos sobrevinientes	2757	según el Informe de PQRSD que comprende el período noviembre de 2024 a febrero de 2025 el Proceso GGOL NO superó la meta de oportunidad del 92%. Su porcentaje de oportunidad de respuesta a las PQRSD fue de 47,72%.

DESCRIPCIÓN RIESGOS MATERIALIZADOS POR PROCESO					
PRIMER CUATRIMESTRE 2025 Trece (14) riesgos materializados					
N°	**Proceso**	**Acta**	**Riesgo Materializado**	**Acción de Mejora**	**Observación**
8	Gestión de la Movilidad	Administrativ-GMOV - 11	Posibilidad de afectación reputacional por Incumplimiento de los términos de Ley para dar respuesta a las PQRSD debido a Demora en las respuestas de PQRSD por parte de los servidores, encargados de atenderlas, dado el gran volumen de estas que llega a la Secretaría de Movilidad	2752	Con la entrada en vigencia de la nueva versión de Mercurio (denominada Mercurio 8.0) se dio lugar a una contingencia en la atención de PQRSD en la Secretaría de Movilidad, dado que toda esta situación administrativa impidió que se atendieran de manera oportuna las PQRSD esperadas. El Indicador de oportunidad se vio afectado y no superó el 92% que se tenía como meta mínima.
9	Gestión de la Obra Pública	SECRETARIA DE INFRAE-GEOP - 63	Posibilidad de afectación económica y reputacional por errores en el análisis de las necesidades y/o en el desarrollo de la factibilidad y/o estructuración de los proyectos de diseño y/o ejecución de obra pública, debido a una inadecuada estimación de alguno de los recursos (humanos, técnicos, financieros, logísticos y/o físicos), o imprecisiones de los estudios, diseños, permisos, licencias, tiempos y/o programación de la ejecución, necesarios para atender las actividades de los proyectos a realizar	5788	En el desarrollo del Proyecto: carrera 43B - No se tenía actualizado el permiso de aprovechamiento forestal por vencimiento de términos y por cambios en las condiciones actuales.
10	Gestión de la Salud	Sec-GESA - 29	Posibilidad de afectación reputacional por inoportunidad en la gestión de PQRSD de la Secretaría de Salud debido a aumento de PQRSD asignadas por temas relacionados con eventos exógenos sobrevinientes (protocolos de bioseguridad)., asignación de PQRSD a servidores que no tenían competencia en el tema, dificultades tecnológicas, tales como fallas en la plataforma y dificultades en la conectividad., insuficiente	2751	"El riesgo se materializó en el primer cuatrimestre de 2025.

DESCRIPCIÓN RIESGOS MATERIALIZADOS POR PROCESO					
PRIMER CUATRIMESTRE 2025 Trece (14) riesgos materializados					
N°	**Proceso**	**Acta**	**Riesgo Materializado**	**Acción de Mejora**	**Observación**
			talento humano para clasificar y direccionar la PQRSD		
11	Gestión de la Seguridad	SEC-GESE - 6	Posibilidad de afectación económica y reputacional por emitir respuestas a las solicitudes de PQRSD que interponen los ciudadanos incumpliendo los requisitos de calidad y los atributos establecidos en la normatividad vigente debido a elaboración y/o entrega de la respuesta de las solicitudes de la ciudadanía (PQRSD) sin el lleno de los atributos de calidad contemplados, los cuales son; respuestas de fondo, claras, congruentes, oportunas y con una notificación eficaz	5309	"Actualmente, se realiza seguimiento al atributo de oportunidad en las respuestas a las solicitudes de PQRSD, con base en los reportes emitidos por el proceso de Atención a la Ciudadanía a través de la plataforma Mercurio. Según el informe más reciente, el indicador GESE presenta un incumplimiento en dicho atributo.
12	Gestión de la Tecnología de la Información y las Comunicaciones	SID-GTIC-17	Posibilidad de afectación económica y reputacional por indisponibilidad de la información producida y recibida en la entidad, debido a Incumplimientos normativos asociados a deficiente implementación de los procesos de la Gestión Documental., Incumplimiento asociado a la prestación de los servicios de las taquillas del Archivo central de la entidad con relación al impacto del Covid- 19, Incumplimientos normativos asociados a la falta de implementación del Plan Institucional de Archivos-PINAR y el Programa de Gestión Documental-PGD., Incumplimientos por factores asociados a la deficiente implementación de la	2740	"Indisponibilidad de la información (componente PQRSD).

DESCRIPCIÓN RIESGOS MATERIALIZADOS POR PROCESO					
PRIMER CUATRIMESTRE 2025 Trece (14) riesgos materializados					
N°	**Proceso**	**Acta**	**Riesgo Materializado**	**Acción de Mejora**	**Observación**
			normatividad sobre Infraestructura Física en los Archivos		
13	Gestión del Control Urbanístico	Sub-GCUR-14	Posibilidad de afectación reputacional por inoportunidad en la gestión de PQRSD de la Secretaría de Salud debido a aumento de PQRSD asignadas por temas relacionados con eventos exógenos sobrevinientes (protocolos de bioseguridad)., asignación de PQRSD a servidores que no tenían competencia en el tema, dificultades tecnológicas, tales como fallas en la plataforma y dificultades en la conectividad., insuficiente talento humano para clasificar y direccionar la PQRSD	2749	"El riesgo SI se materializa.
14	Gestión del Riesgo de Desastres	DEPTO. GRED-GRDD114	Posibilidad de afectación reputacional por Incumplimiento en la prestación del servicio debido a Inoportunidad en la gestión de las PQRSD del proceso, Inoportunidad en la prestación del servicio de atención de emergencias, Inexactitud en la información estratégica - POT y operativa para la toma de decisiones en las inspecciones por riesgo, Evento exógeno sobreviniente	2755	Por exceder el límite de tolerancia en la oportunidad de respuesta de las PQRSD asociadas al proceso GRDD