Alcaldía de Medellín
Distrito de
Ciencia, Tecnología e Innovación

SISTEMA INTEGRAL DE GESTIÓN - SIG

INFORME ADMINISTRACIÓN DE RIESGOS DE GESTIÓN

Segundo Cuatrimestre 2025
Abril 01 al 31 de julio 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
Agosto 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 Abril 01 al 31 de julio 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 abril 01 y 31 de julio 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 – SEGUNDO 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 del 01 de abril de 2025, la distribución de los riesgos de gestión y de corrupción, fue la siguiente:

Tipo Riesgo	Total Riesgos
Corrupción	68
Gestión	106
Total general	**174**

Gráfica 1 Tipo de riesgos VS Total de Riesgos

La gráfica 1 evidencia la identificación de ciento setenta y un (174) riesgos distribuidos en los veintisiete (27) procesos, de los cuales ciento seis (106) riesgos son de gestión y representan un sesenta y uno por ciento (61%), y sesenta y ocho (68) riesgos son de corrupción que equivalen a un treinta y nueve (39%) 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 de la Salud	7
Gestión del Desarrollo Económico	7
Gestión de la Obra Pública	6
Gestión de la Tecnología de la Información y las Comunicaciones	6
Administración de Bienes Muebles e Inmuebles	5
Evaluación y Mejora Institucional	5
Gestión de la Seguridad	5
Servicio a la Ciudadanía	5
Gestión del Riesgo de Desastres	4
Fortalecimiento de la Ciudadanía	3
Gestión Ambiental	3
Gestión Cultural	3
Gestión de la Educación	3
Gestión de la Información	3
Gestión de Servicios Públicos Domiciliarios y No Domiciliarios	3
Gestión Integral del Talento Humano	3
Gestión Jurídica	3
Comunicación Pública	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
Gestión Catastral	1
Mantenimiento de Bienes Muebles e Inmuebles	1
Total general	106

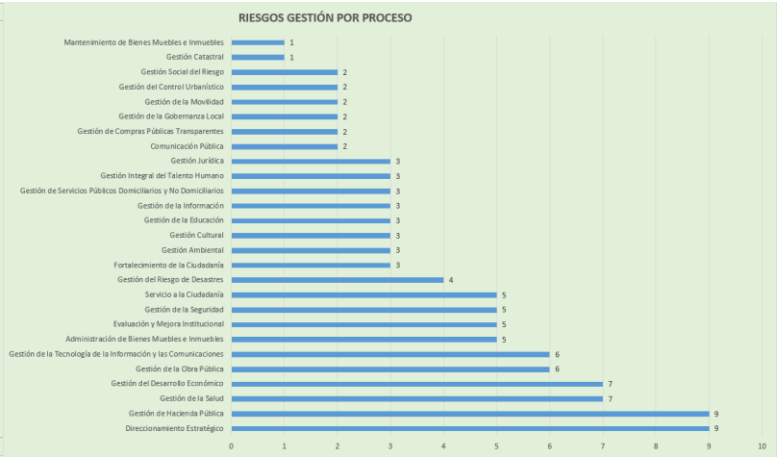


Tabla 1. Cantidad riesgos de gestión por proceso

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

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 cuatro por ciento (64%) 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 segundo cuatrimestre del 2025, se evidencia que hubo una variación de un 3% en los riesgos de gestión como se muestra en la siguiente grafica:

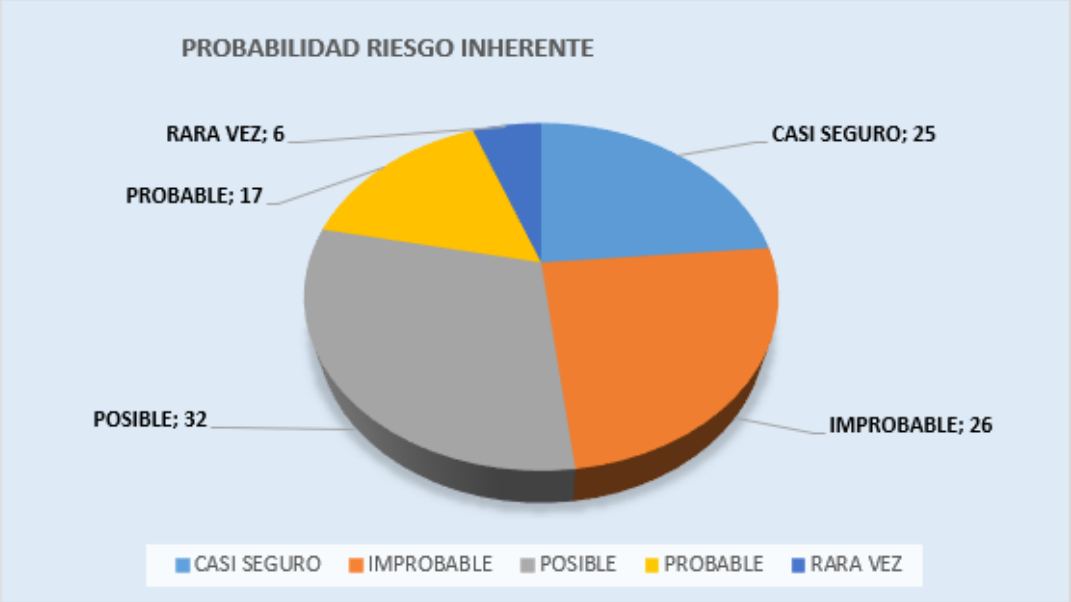
Proceso	Cantidad de Riesgos de Gestión		
	1er Cuatrimestre 2025	2do Cuatrimestre 2025	Variación
Administración de Bienes Muebles e Inmuebles	4	5	1
Comunicación Pública	2	2	0
Direccionamiento Estratégico	9	9	0
Evaluación y Mejora Institucional	5	5	0
Fortalecimiento de la Ciudadanía	3	3	0
Gestión Ambiental	4	3	-1
Gestión Catastral	2	1	-1
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	6	3
Gestión de la Salud	6	7	1
Gestión de la Seguridad	5	5	0
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	**103**	**106**	**3**
Variación Porcentual	**3%**		

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

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*:

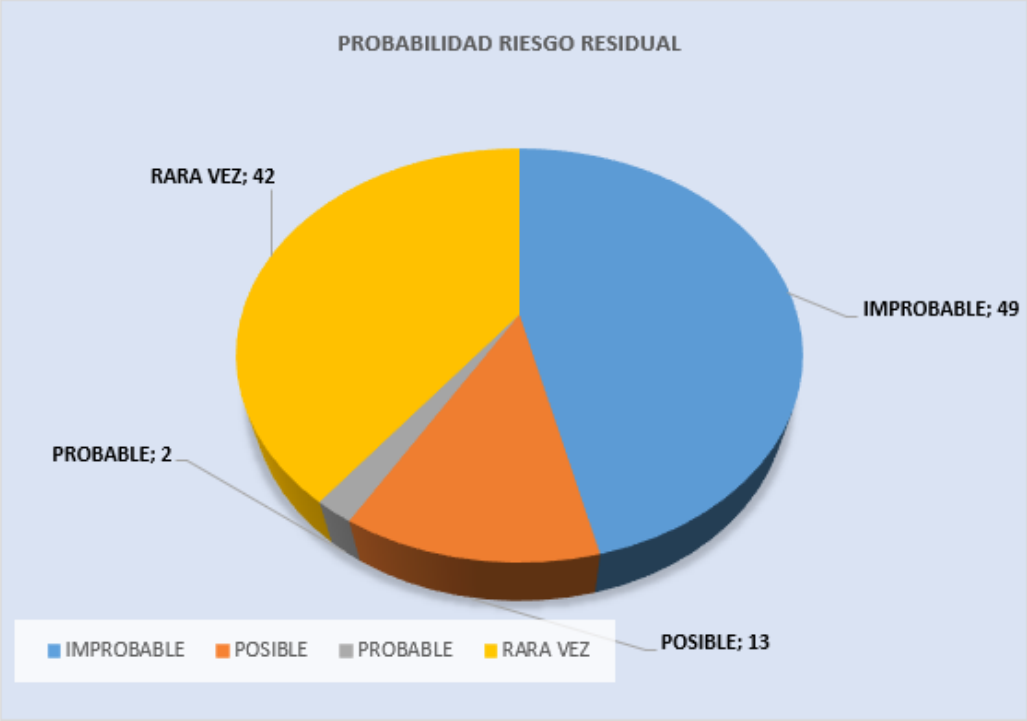
PROBABILIDAD RIESGO INHERENTE	Total
CASI SEGURO	25
IMPROBABLE	26
POSIBLE	32
PROBABLE	17
RARA VEZ	6
Total general	**106**



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	49
POSIBLE	13
PROBABLE	2
RARA VEZ	42
Total general	**106**



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 seis (106) *riesgos de gestión* definidos en la entidad, se diseñaron un total de doscientos cincuenta (250) controles, que se clasifican en controles preventivos (56 %), detectivos (39%) y correctivos (5%).

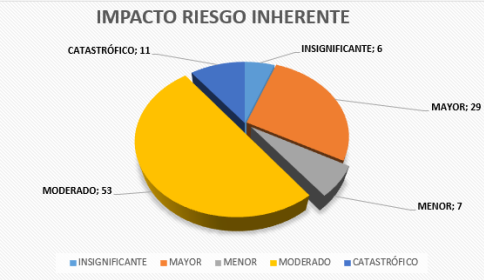
NATURALEZA DEL CONTROL RIESGOS GESTIÓN	
DESCRIPCIÓN DEL CONTROL	Total Controles
Detectivo	98
Preventivo	140
Correctivo	14
Total general	**252**

Gráfica 4 Descripción del Control vs Total Controles

5.6 Zona de impacto riesgo inherente y residual

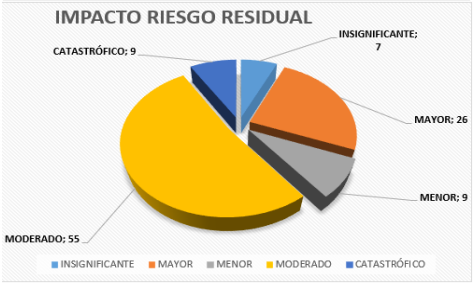
Acorde con lo establecido en la metodología utilizada por parte del Distrito de Medellín para la administración del riesgo, a los riesgos de gestión les aplica los niveles de impacto “Insignificante”, “Menor”, “Moderado”, “Mayor” y “Catastrófico. Así mismo se establece que con la ejecución de controles 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	53
CATASTRÓFICO	11
Total general	**106**



Gráfica 5 Zona inherente riesgo de gestión

IMPACTO RIESGO RESIDUAL POR ZONA	Total Riesgos
INSIGNIFICANTE	7
MAYOR	26
MENOR	9
MODERADO	55
CATASTRÓFICO	9
Total general	**106**



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	28
BAJO	10
EXTREMO	9
MODERADO	59
Total general	**106**

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 (28) y moderado (59) que equivalen al 91%, deben contar con controles que permitan REDUCIR la probabilidad de ocurrencia del riesgo.

5.8 Riesgos de gestión materializados

Para el segundo 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 marzo a junio 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.

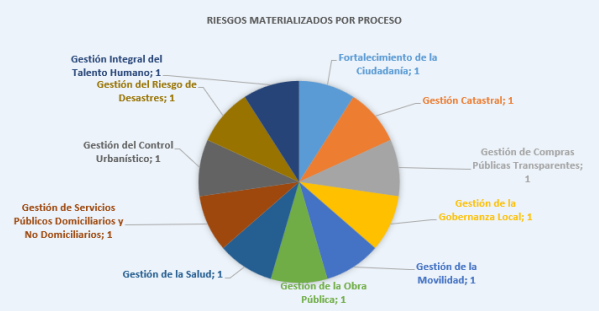
De los ciento seis (106) riesgos de gestión identificados en los veintisiete (27) procesos, durante el segundo cuatrimestre se evidencia la materialización de once (11) riesgos, como lo muestra la gráfica 8.

RIESGOS MATERIALIZADOS	
Materializó	**Total**
No	95
Si	11
Total general	**106**

Gráfica 8 Materialización riesgos de gestión

Los *riesgos de gestión* materializados (11), se distribuyeron en once (11) de los veintisiete (27) procesos, tal y como se presenta en la gráfica 9; dichos procesos materializaron de a un riesgo:

RIESGOS MATERIALIZADOS	
PROCESO	Total
Fortalecimiento de la Ciudadanía	1
Gestión Catastral	1
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 Servicios Públicos Domiciliarios y No Domiciliarios	1
Gestión del Control Urbanístico	1
Gestión del Riesgo de Desastres	1
Gestión Integral del Talento Humano	1
Total general	**11**



Gráfica 9 Riesgos materializados por proceso

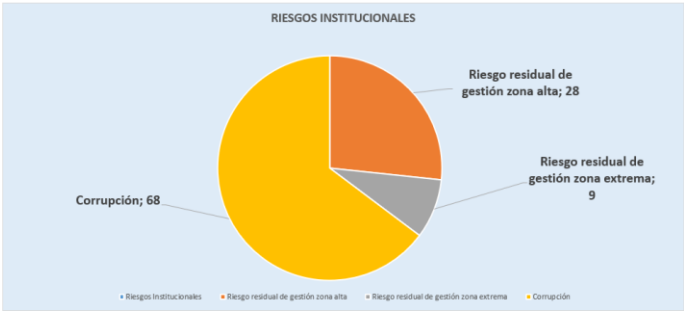
En el anexo 1 *Descripción Riesgos Materializados Por Proceso,* se encuentran los riesgos materializados, clasificados por proceso, el acta que evidencia la autoevaluación, la acción de mejora formulada por parte de los directivos que lideran procesos en conjunto con sus equipos, con el fin de mitigar 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	28
Riesgo residual de gestión zona extrema	9
Corrupción	68
Total general	**105**



Gráfica 10 Riesgos Institucionales

En la tabla 4 (riesgos de gestión en zona alta, 28 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

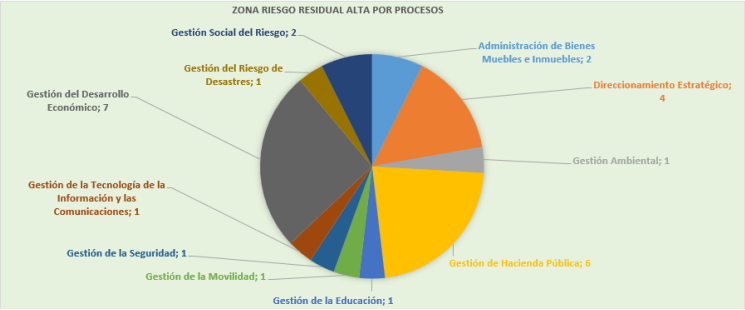


Tabla 4. Zona de riesgo residual alta

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

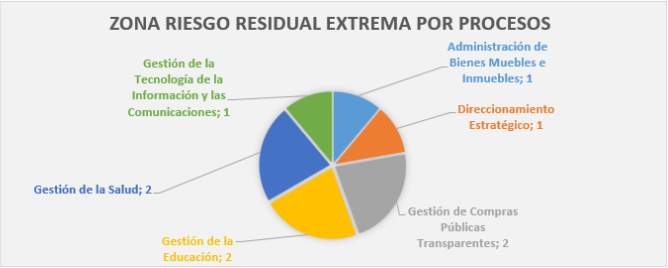


Tabla 5. Zona de riesgo residual extrema

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 continúa siendo un pilar estratégico esencial para anticipar y mitigar situaciones que puedan comprometer el cumplimiento de los objetivos institucionales. En un entorno cada vez más interconectado y digitalizado, cualquier incidente ya sea directo o indirecto puede impactar la continuidad de los procesos organizacionales, afectar la calidad de los servicios prestados o incluso derivar en incumplimientos críticos.

En este sentido, la identificación, evaluación y monitoreo de los riesgos asociados a la seguridad de la información y la ciberseguridad ahora integrados bajo el concepto más amplio de seguridad digital representan una herramienta clave para una gestión informada y proactiva. Este enfoque, respaldado por lineamientos como la Guía para la Gestión del Riesgo y el diseño de controles del Departamento Administrativo de la

Función Pública, así como por la Política de Gobierno Digital del Ministerio TIC, permite a las entidades orientar la inversión, priorizar acciones y fortalecer capacidades en función de los riesgos reales que enfrentan.

En este contexto, se presenta el seguimiento a la materialización de riesgos frente a ciberamenazas, los cuales han sido identificados, analizados y valorados por la Unidad de Seguridad Informática. Este informe abarca el periodo comprendido entre abril de 2025 y julio de 2025, y constituye una herramienta para la toma de decisiones estratégicas en materia de ciberseguridad organizacional.

Contexto de los Riesgos Frente a Ciberamenazas

Para comprender el análisis y seguimiento realizado durante el último cuatrimestre a los riesgos asociados a ciberamenazas, es necesario contextualizar que, a nivel mundial, las amenazas digitales evolucionan constantemente en complejidad y frecuencia, afectando tanto a sectores privados como a gobiernos locales. En ese marco, la Alcaldía de Medellín, como entidad pública responsable de múltiples servicios esenciales, no es ajena a estas dinámicas globales y debe actuar con un enfoque preventivo y adaptativo.

Desde la Unidad de Seguridad Informática, se han identificado y valorado los principales riesgos que podrían comprometer la disponibilidad, integridad y confidencialidad de los activos tecnológicos de la entidad. A partir de este análisis, se establece un conjunto de riesgos priorizados que definen el enfoque estratégico y el alcance del seguimiento realizado en el periodo comprendido, permitiendo así orientar los esfuerzos institucionales frente a un panorama digital cada vez más desafiante:

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.

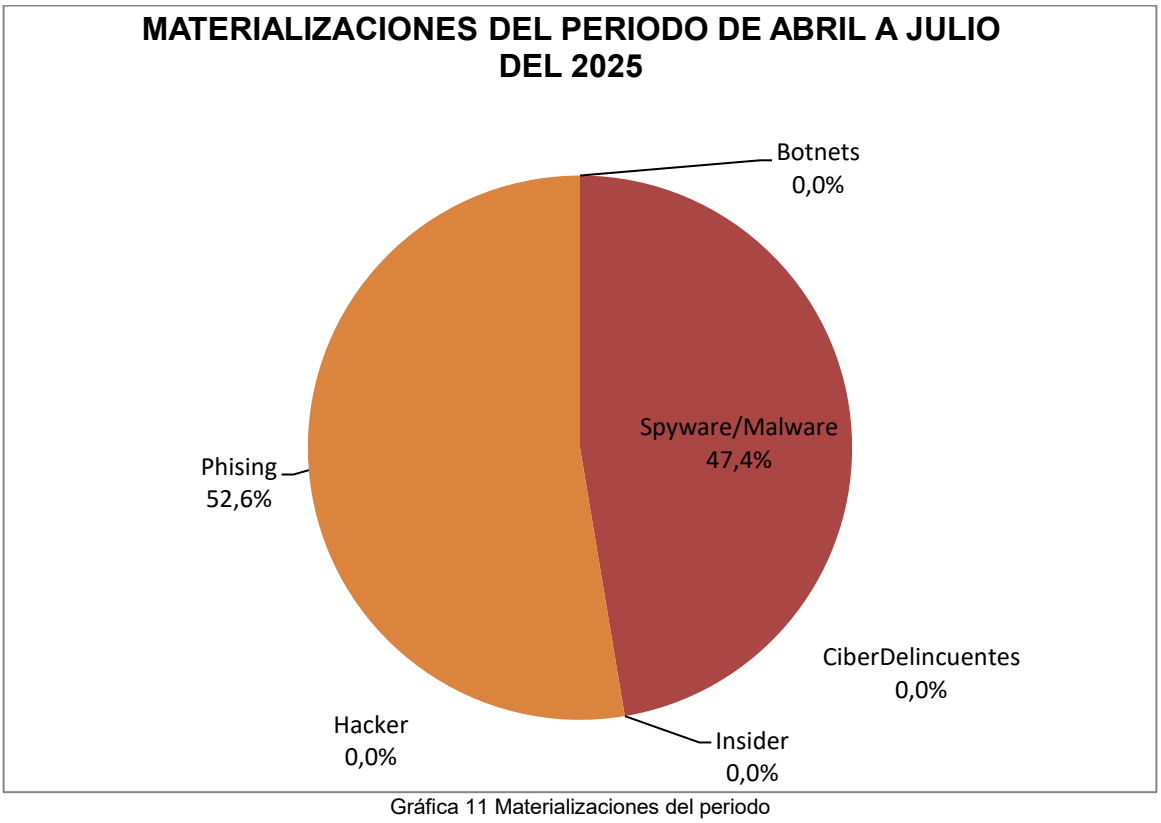
En concordancia con los riesgos previamente identificados y valorados, se presenta a continuación el detalle de las materializaciones ocurridas durante el periodo de análisis, estructuradas en la siguiente tabla. Esta información permite evidenciar el impacto real de las amenazas sobre los activos tecnológicos 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	8
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	10
	TOTAL DE MATERIALIZACIONES	19

Tabla 7. Afectación de la Disponibilidad

El total de materializaciones en el periodo fue de 19 en relación con los grupos de riesgos identificados, de los cuales el 47,4% están relacionados con Spyware/Malware que ha afectado equipos de usuario final y el 52.6 % está relacionado con phishing en correo Electrónico Institucional. Tal como se puede apreciar en la siguiente gráfica:

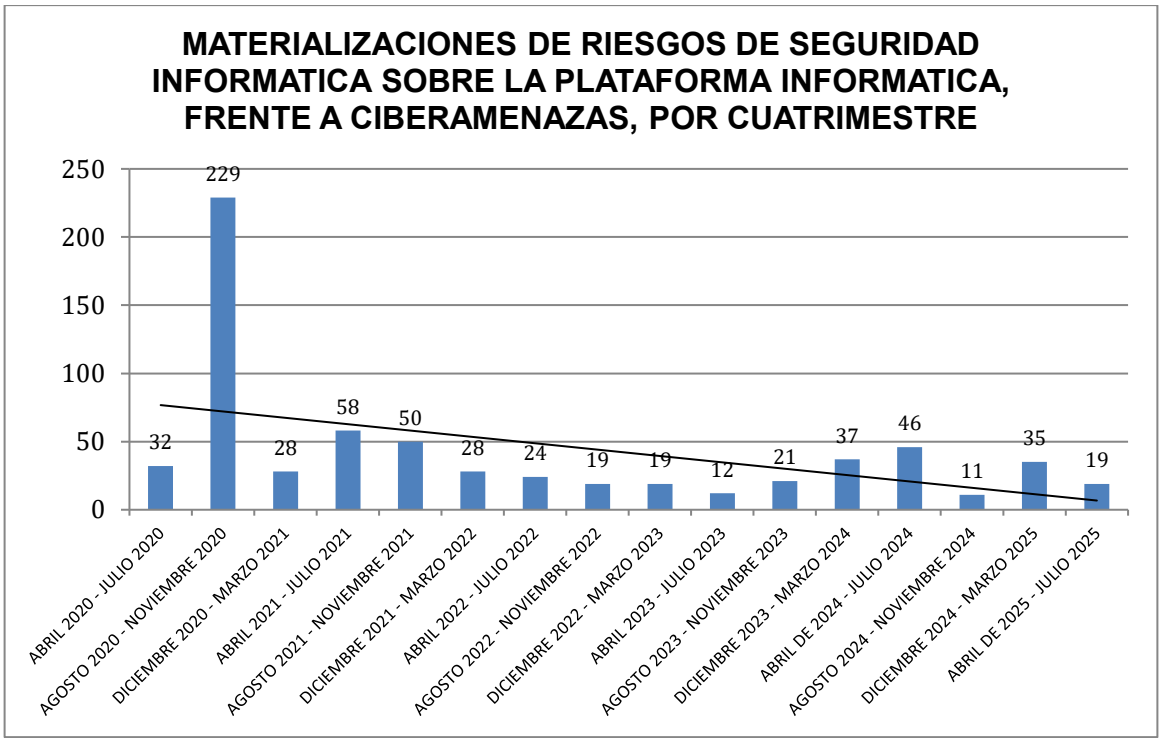


Gráfica 11 Materializaciones del periodo

ANALISIS POR FUENTE DE AMENAZAS EN EL PERIODO ABRIL – JULIO 2025	
Amenazas	Materializaciones
Botnets	0
Spyware/Malware	9
Hacker	0
Insider	0
CiberDelincuentes	0
Phishing	10
TOTAL	19

Tabla 8. Análisis por fuente de amenazas en el periodo

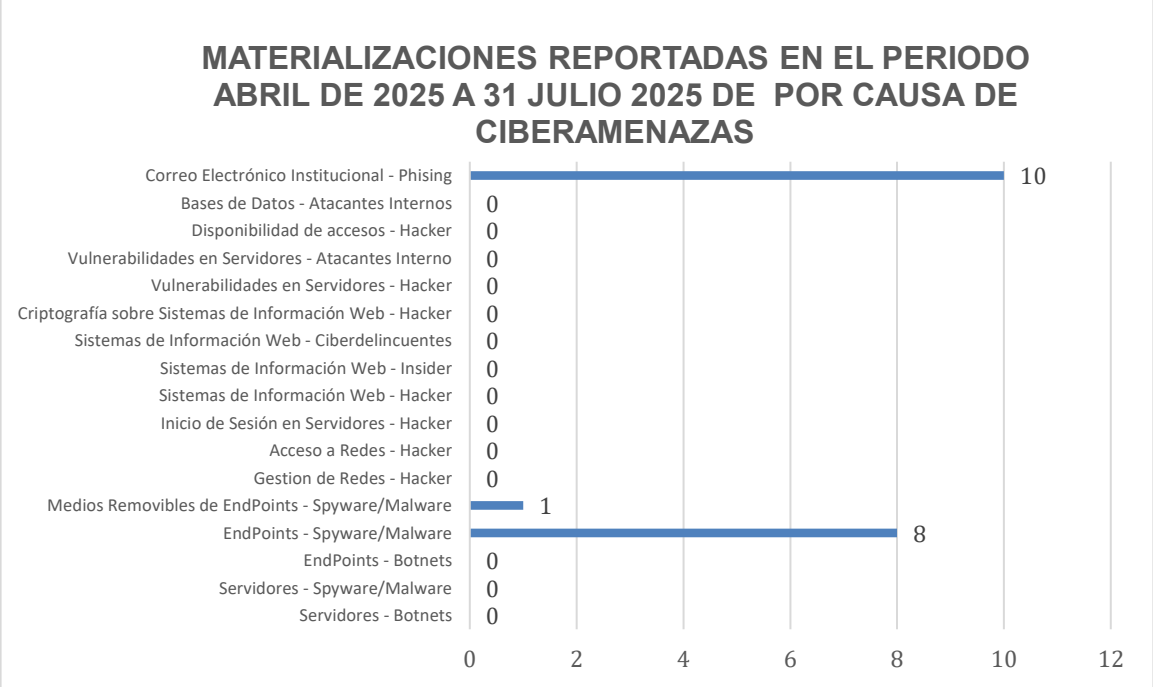
Se puede observar referente a las materializaciones que se evidencia una disminución del 45.7% en comparación con las materializaciones del cuatrimestre anterior, tal como se presenta en la siguiente gráfica:



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 42,10% de los casos correspondieron a malware en estaciones de usuario final, seguido de un 5,26% por infección a través de medios removibles. Así mismo, se identificaron materializaciones de phishing en el correo electrónico institucional que representaron un 52,63% 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 en ciberseguridad dentro 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 digital.

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 segundo 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 cincuenta y dos (252) 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 seis (106) riesgos de gestión identificados en los veintisiete (27) procesos, se evidencia la materialización de 11 riesgos, correspondiente al 10% del universo de riesgos de gestión de la entidad.

- Para el segundo cuatrimestre del año 2025 hubo cambios en el número de riesgos de gestión de la entidad con respecto a los autoevaluados en el primer cuatrimestre de la vigencia 2025; hubo un incremente de 3 riesgos equivalente al 3%.

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					
SEGUNDO CUATRIMESTRE 2025 Trece (11) riesgos materializados					
N°	**Proceso**	**Acta**	**Riesgo Materializado**	**Acción de Mejora**	**Observación**
1	Gestión de Compras Públicas Transparentes	Sec-GEC-39	Posibilidad de afectación económica y reputacional por 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 debido a inaplicación de los procedimientos en el desarrollo del proceso.	2765	Secretaría de Innovación Digital La materialización de este riesgo se dio porque en el periodo comprendido entre el 16 de marzo de 2025 y el 15 de julio de 2025, la Secretaría de Innovación Digital informó que en el proceso contractual que se adelantó por la modalidad de Licitación Pública número 70007686 de 2025, que tuvo por objeto: “Adquirir los Servicios de Apoyo Tecnológico a la Plataforma Informática del Distrito de Medellín”, se realizó una inadecuada estructuración de los requisitos técnicos (experiencia), ocasionando que ningún oferente pudiera cumplir y el proceso fuera declarado desierto el 30 de abril de 2025. Causa: Inaplicación de los procedimientos en el desarrollo del proceso, por una inadecuada estructuración de los requisitos técnicos (experiencia), se presentaron múltiples observaciones en dicho sentido que desde lo jurídico era imposible apoyar por ser temas técnicos, ocasionando que ningún oferente pudiera cumplir y el proceso fuera declarado desierto el 30 de abril de 2025.
2	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	2722	Se presentó incumplimiento en la oportunidad de respuesta del 37% de los 5,156 trámites ingresados en el periodo de 01 de abril de 2024 al 31 de julio de 2025; se tienen 11,616 solicitudes pendientes correspondientes al corte del 01 de agosto de 2025. El tiempo promedio de respuesta de las solicitudes durante el periodo a analizar fue de 172,08 días. El riesgo se materializó debido al alto volumen de trámites que se

DESCRIPCIÓN RIESGOS MATERIALIZADOS POR PROCESO					
SEGUNDO CUATRIMESTRE 2025 Trece (11) riesgos materializados					
N°	**Proceso**	**Acta**	**Riesgo Materializado**	**Acción de Mejora**	**Observación**
			ejecución contractual por parte del tercero de apoyo a la gestión catastral, Represamiento de tramites, Evento fortuito sobreviniente de las inundaciones, deslizamiento, altas temperaturas, daños a la infraestructura que impidan la verificación en el campo		encontraban represados y que no fue posible atender en su totalidad. No obstante, se están implementando diferentes estrategias con el fin de ponerse al día en la atención y respuesta de dichos trámites.
3	Gestión del Control Urbanístico	Sub-GCUR-15	Posibilidad de afectación reputacional por Inoportunidad en la entrega de las respuestas a las solicitudes de los ciudadanos y dependencias del distrito de Medellin, relacionadas con los procesos constructivos y monitoreos de ciudad. debido a Alto volumen de solicitudes internas y externas, que evidencian cargas laborales inequitativas , y a evento exógeno sobreviniente (pandemias, emergencias sanitarias, desastres naturales, cambio climático, otros eventos de impacto nacional y mundial), , ,	2749	Aunque se ha mejorado los controles para el seguimiento de las PQRSD, en la Subsecretaria el alto volumen que ingresa de solicitudes como oficios, PQRSD, solicitudes por órganos de control, es alto. En contraste con los limitados recursos disponibles. No obstante en este periodo evaluado de los 1416, los oportunos fueron 1289 equivalentes al 91,03% y los no oportunos 127 equivalentes al 8,97% fueron respondidas en un mayor %, en tiempos muy cercano a la fecha de respuesta limite, además aunque la plataforma de Mercurio ha ido mejorando, en los primeros meses del año estuvo bastante compleja la situación con la plataforma y actualmente lo que también en muchas ocasiones afecta a los profesionales dar incluso respuestas oportunas, por fallas de la plataformas muchas salen no oportunas. Los controles si han minimizado los tiempos de respuestas, y se continuará con la aplicación de los controles que se vienen realizando. Se tiene Acción para abordar riesgos #2749 en Isolución para dar cobertura a la materialización de este riesgo en la vigencia 2025. Según reporte entregado por Servicio a la Ciudadanía de las PQRSD responsabilidad del proceso de Control Urbanístico, se tiene el siguiente detalle del número de solicitudes respondidas inoportunamente:

DESCRIPCIÓN RIESGOS MATERIALIZADOS POR PROCESO					
SEGUNDO CUATRIMESTRE 2025 Trece (11) riesgos materializados					
N°	**Proceso**	**Acta**	**Riesgo Materializado**	**Acción de Mejora**	**Observación**
					Total PQRSD Marzo a Junio 2025 = 1.416=100% Total PQRSD gestionadas oportunamente= 1.289 = 91.03% Total PQRSD gestionadas inoportunamente = 127= 8.97% Este detalle comprende el periodo entre Marzo y Junio de 2025 toda vez que Según el Decreto 491 de 2020, establece en su artículo 5 “Ampliación de términos para atender las peticiones”.
4	Fortalecimiento de la Ciudadanía	SECRETARIA DE PARTIC-FOCI -102	Posibilidad de afectación económica y reputacional por incumplimiento o ejecución inoportuna en la entrega de bienes o la prestación de trámites, servicios o PQRSD, requeridos para el desarrollo de las estrategias de formación, participación democrática, movilización, organización y control social. debido a falta de alineación entre los tiempos de ejecución institucional y los ciclos de participación (por ejemplo, cronograma ruta de presupuesto participativo o de los planes de desarrollo local)., desarticulación entre las áreas responsables de la ejecución, Retrasos en la contratación logística, de apoyo a la gestión o técnica.,	2764	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. Durante el período de autoevaluación, y pese a la existencia de controles previamente definidos, se materializó el riesgo de incumplimiento en dos frentes principales: 1. Atención a PQRS: Se evidenció falta de oportunidad en la respuesta, lo que afecta la satisfacción ciudadana y el cumplimiento normativo. De 400 ingresadas en el período de la autoevaluación, 33 no fueron oportunas, lo que corresponde al 8.25%, superando el 92% de tolerancia permitido 2. Indicadores de producto: Los resultados obtenidos en los indicadores 3.2.2.6 (34,7%), 3.2.3.4 (11,6%) y 3.2.1.10 (24,7%) fueron inferiores al umbral mínimo del 45% establecido para la fecha de corte (30 de junio de 2025). Esto refleja rezagos en la ejecución física de las metas, con un avance global del 39% con ubicación en zona de semaforización amarilla. Por lo tanto, fué necesario tomar medidas correctivas para subsanar estas deficiencias.

DESCRIPCIÓN RIESGOS MATERIALIZADOS POR PROCESO					
SEGUNDO CUATRIMESTRE 2025 Trece (11) riesgos materializados					
N°	**Proceso**	**Acta**	**Riesgo Materializado**	**Acción de Mejora**	**Observación**
5	Gestión Integral del Talento Humano	Sub-GETH - 18	Posibilidad de afectación económica y reputacional por incumplimiento en la gestión del talento humano que impacte el cumplimiento de los objetivos de la entidad, debido a modificación de políticas normas y directrices desde el nivel nacional y por cambios de administración, falta de recursos humanos, financieros y logísticos, tecnología y sistemas de información que no responden a las necesidades del proceso, inexactitud y/o inexistencia en la información de la Base de Datos de la Entidad, enviada al Grupo PASIVOCOL del Ministerio de Hacienda y Crédito Público, Incumplimiento por evento exógeno con efectos de cambio climático	2766	64 PQRSD inoportunas, de 579 en total (oportunas 515 y no oportunas 64), para un porcentaje de inoportunidad del 11.05%. En el resto de los controles se evidenció que se cumplió con las actividades propuestas en cada uno de los programas/proyectos/estrategias, lo que ha permitido la continuación del proceso, pese a las dificultades señaladas mediante las distintas alertas allegadas de manera oportuna. Se informó los casos donde se hacen evidentes la necesidad de recursos financieros, logísticos y tecnológicos, ante las dependencias respectivas, no obstante, se continuó con la operación del proceso. Se ha procurado por mantener la efectividad de las herramientas tecnológicas y sistemas de información, mediante el repote oportuno de las necesidades de desarrollo, etc. Se envío base de datos de la entidad depurada y revisada al Grupo PASIVOCOL del Ministerio de Hacienda y Crédito Público de la Base de Datos de la Entidad y se acatan observaciones.
6	Gestión de la Obra Pública	SECRETARIA DE INFRAE-GEOP - 67	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 impresiones de los estudios, diseños, permisos,	5788	En el Lazo descenso palmas - no se diseñó un box Colbert – En el Lazo ascenso palmas se hizo un mal diseño de un puente y para los puentes de la Q. hueso y Q. pelahueso no se diseñaron redes secas ni redes húmedas.”

DESCRIPCIÓN RIESGOS MATERIALIZADOS POR PROCESO					
SEGUNDO CUATRIMESTRE 2025 Trece (11) riesgos materializados					
N°	**Proceso**	**Acta**	**Riesgo Materializado**	**Acción de Mejora**	**Observación**
			licencias, tiempos y/o programación de la ejecución, necesarios para atender las actividades de los proyectos a realizar, , , ,		
7	Gestión de la Gobernanza Local	Sec-GGOL-55	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, de tipo biológico o eventos asociados al cambio climático como inundaciones, incendios, desastres naturales, que afectan la atención.	2757	según el Informe de PQRSD que comprende el período marzo a junio de 2025 el Proceso GGOL NO superó la meta de oportunidad del 92%. Su porcentaje de oportunidad de respuesta a las PQRSD fue de 69,29%.
8	Gestión del Riesgo de Desastres	DEPTO. DEP-GRDD - 21	Posibilidad de afectación económica y reputacional por Incumplimiento de los términos legales en razón a la atención de PQRSD emitidas por los ciudadanos. debido a Insuficiente capacidad instalada para dar respuestas a las solicitudes (PQRSD).	2755	Por exceder el límite de tolerancia en la oportunidad de respuesta de las PQRSD asociadas al proceso GRDD.

DESCRIPCIÓN RIESGOS MATERIALIZADOS POR PROCESO					
SEGUNDO CUATRIMESTRE 2025 Trece (11) riesgos materializados					
N°	**Proceso**	**Acta**	**Riesgo Materializado**	**Acción de Mejora**	**Observación**
9	Gestión de la Movilidad	Unidad Administrativ-GMOV-12	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	Según informe de Servicio a la Ciudadanía de PQRSD de Marzo a Junio de 2025 por la Secretaría de Movilidad no se logró la meta de oportunidad del 92%.
10	Gestión de la Salud	Sec-GESA - 32	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, asociados a cambios climáticos)., 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 ,	2751	En cuanto a la oportunidad en la respuesta: Se registraron 2.646 casos de respuestas oportunas, lo que representa el 48 % del total. Se evidencia una tendencia creciente en la oportunidad de respuesta, pasando de un 16,4 % en marzo a un 76,92 % en junio. Se registraron 3.031 casos de respuestas no oportunas, lo que representa el 52 % del total. Se observa una reducción significativa mes a mes, pasando de 1.357 casos en marzo a 264 en junio. Es importante señalar que, de las 3.031 PQRSD respondidas de manera inoportuna, 2.955 casos (equivalente al 97,49 %) corresponden al área de Salud Ambiental.
11	Gestión de Servicios Públicos Domiciliarios y No Domiciliarios	Sec-GSPD - 34	Posibilidad de afectación económica y reputacional por Inexactitud en la formulación de un proyecto por deficiencias en los cálculos financieros de proyecciones que soportan una inversión debido a Estimaciones o presupuestos basados en información proyectada con variables no predecibles como la inflación, las tasas de interés, TMR,, IPP (Índice de	2771	Según lo establecido en el preinforme de la Auditoria Especial a la contratación de Acueducto y alcantarillado, se presentaron falencias en los alcances a los objetivos contractuales de los procesos 2018, 2019 y 2020

DESCRIPCIÓN RIESGOS MATERIALIZADOS POR PROCESO					
SEGUNDO CUATRIMESTRE 2025 Trece (11) riesgos materializados					
N°	**Proceso**	**Acta**	**Riesgo Materializado**	**Acción de Mejora**	**Observación**
			precios al Productor), actualización tarifaria., Falta de personal vinculado en cantidad y especialidad de conocimientos para ejercer la supervisión., Desarticulación entre los componentes involucrados para la estructuración y ejecución de los proyectos.,		