Alcaldía de Medellín
Distrito de
Ciencia, Tecnología e Innovación

SISTEMA INTEGRAL DE GESTIÓN - SIG

INFORME ADMINISTRACIÓN DE RIESGOS DE GESTIÓN

Tercer Cuatrimestre 2024
Agosto a noviembre de 2024

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
Diciembre de 2024

TABLA DE CONTENIDO

INTRODUCCIÓN
1. FUNDAMENTO NORMATIVO
2. OBJETIVO
3. ALCANCE
4. ASPECTOS GENERALES
   4.1. Metodología
   4.2. Modelo de Operación
5. ESTADO DE LOS RIESGOS DE GESTIÓN – TERCER CUATRIMESTRE 2024
   5.1 Universo riesgos (corrupción y gestión)
   5.2 Distribución Riesgos de Gestión por proceso
   5.3 Variación riesgos de gestión
   5.4 Probabilidad de ocurrencia
   5.5 Naturaleza del control en los riesgos de gestión
   5.6 Zona de impacto riesgo inherente y residual
   5.7 Zona de riesgo residual
   5.8 Riesgos de gestión materializados
6. RIESGOS INSTITUCIONALES
   6.1 Riesgos Institucionales
7. SEGUIMIENTO RIESGOS SEGURIDAD INFORMÁTICA
8. Seguimiento a los Riesgos de seguridad informática identificados y sus materializaciones.
9. CONCLUSIONES
10. RECOMENDACIONES
ANEXO 1

LISTA DE ILUSTRACIONES

Ilustración 1. Modelo de Operación por Procesos
Ilustración 2. Categorización que la solución antimalware
Ilustración 3. Efectividad del control implementado

LISTA DE TABLAS

Tabla 1. Cantidad riesgos de gestión por proceso
Tabla 2. Procesos mayor cantidad de riesgos de gestión
Tabla 3. Variación riesgos de gestión
Tabla 4. Zona de riesgo residual alta
Tabla 5. Zona de riesgo residual extrema
Tabla 6. Agrupación de los Riesgos de Seguridad Informática
Tabla 7. Afectación de la Disponibilidad
Tabla 8. Análisis por fuente de amenazas en el periodo

LISTA DE GRÁFICAS

Gráfica 1 Tipo de riesgos VS Total de Riesgos
Gráfica 2 Probabilidad de ocurrencia riesgos inherentes
Gráfica 3 Probabilidad ocurrencia riesgo residual
Gráfica 4 Descripción del Control vs Total Controles
Gráfica 5 Zona inherente riesgo de gestión
Gráfica 6 Zona residual riesgos de gestión
Gráfica 7 Zona de riesgo residual
Gráfica 8 Materialización riesgos de gestión
Gráfica 9 Riesgos materializados por proceso
Gráfica 10 Riesgos Institucionales
Gráfica 11 Materializaciones del periodo
Gráfica 12 Clasificación Materializaciones del periodo
Gráfica 13 Materializaciones en el periodo

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 a julio de 2024.

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 segundo cuatrimestre comprendido entre agosto y noviembre de 2024, 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 – TERCER CUATRIMESTRE 2024

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 30 de noviembre de 2024, la distribución de los riesgos de gestión y de corrupción, fue la siguiente:

Tipo Riesgo	Total Riesgos
Corrupción	65
Gestión	101
Total general	**166**

Gráfica 1 Tipo de riesgos VS Total de Riesgos

La gráfica 1 evidencia la identificación de ciento sesenta y seis (166) riesgos distribuidos en los veintisiete (27) procesos, de los cuales ciento un (101) riesgos son de gestión y representan un sesenta y un por ciento (61%), y sesenta y cinco (65) 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 un (101) riesgos de gestión identificados a corte 30 de noviembre de 2024, se distribuyen en los veintisiete (27) procesos del Modelo de Operación, de la siguiente manera:

PROCESO	Total Riesgos
Mantenimiento de Bienes Muebles e Inmuebles	1
Comunicación Pública	2
Gestión Catastral	2
Gestión de la Gobernanza Local	2
Gestión de la Movilidad	2
Gestión del Control Urbanístico	2
Gestión Social del Riesgo	2
Fortalecimiento de la Ciudadanía	3
Gestión Cultural	3
Gestión de Compras Públicas Transparentes	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
Administración de Bienes Muebles e Inmuebles	4
Gestión Ambiental	4
Gestión de la Seguridad	4
Gestión del Riesgo de Desastres	4
Servicio a la Ciudadanía	4
Evaluación y Mejora Institucional	5
Gestión de la Tecnología de la Información y las Comunicacion	5
Gestión de la Salud	6
Gestión del Desarrollo Económico	7
Direccionamiento Estratégico	9
Gestión de Hacienda Pública	9
Total general	101

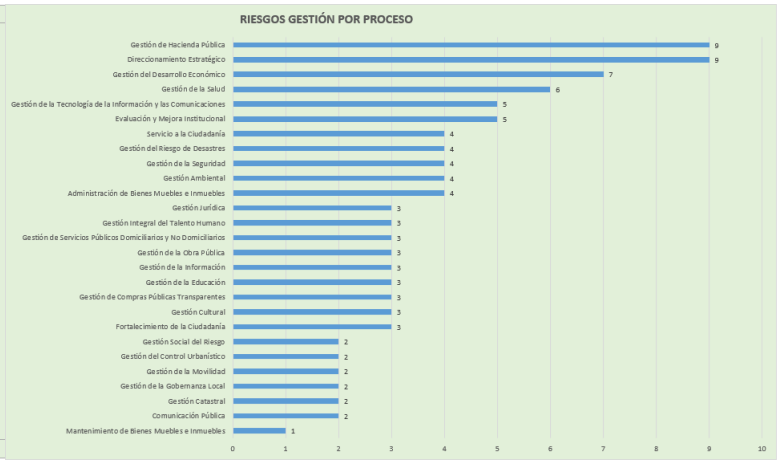


Tabla 1. Cantidad riesgos de gestión por proceso

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	5
Evaluación y Mejora Institucional	5
Administración de Bienes Muebles e Inmuebles	4 (en cada proceso)
Gestión Ambiental	
Gestión del Riesgo de Desastres	
Gestión de la Seguridad	
Servicio a la Ciudadanía	

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 por ciento (60%) 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 autoevaluados en el segundo cuatrimestre de 2024 con la autoevaluación del primer cuatrimestre del 2024, se evidencia que no hubo variación, como lo indica la siguiente tabla:

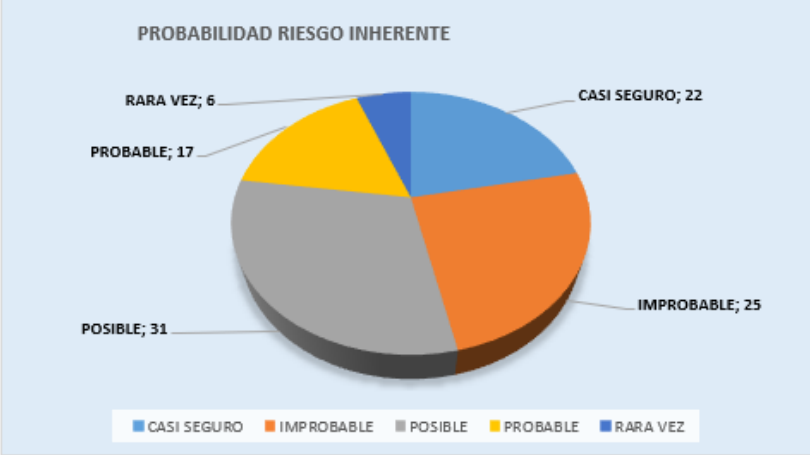
Proceso	Cantidad de Riesgos de Gestión		
	2do Cuatrimestre 2024	3er Cuatrimestre 2024	Variación
Administración de Bienes Muebles e Inmuebles	4	4	0
Comunicación Pública	2	2	0
Direccionamiento Estratégico	9	9	0
Evaluación y Mejora Institucional	5	5	0
Fortalecimiento de la Ciudadanía	3	3	0
Gestión Ambiental	4	4	0
Gestión Catastral	2	2	0
Gestión Cultural	3	3	0
Gestión de Compras Públicas Transparentes	3	3	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	4	0
Gestión de la Tecnología de la Información y las Comunicacion	5	5	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	4	4	0
Total Riesgos por Cuatrimestre	**101**	**101**	**0**
Variación Porcentual	**0%**		

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*:

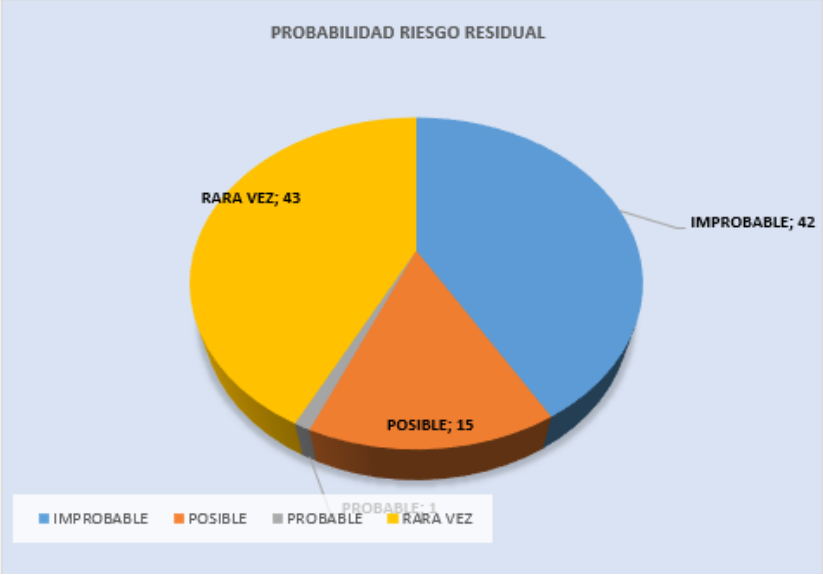
PROBABILIDAD RIESGO INHERENTE	Total
CASI SEGURO	22
IMPROBABLE	25
POSIBLE	31
PROBABLE	17
RARA VEZ	6
Total general	**101**



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	42
POSIBLE	15
PROBABLE	1
RARA VEZ	43
Total general	**101**



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 un (101) *riesgos de gestión* definidos en la entidad, se diseñaron un total de doscientos cuarenta y dos (242) controles, que se clasifican en controles preventivos (57%), detectivos (38%) y correctivos (5%).

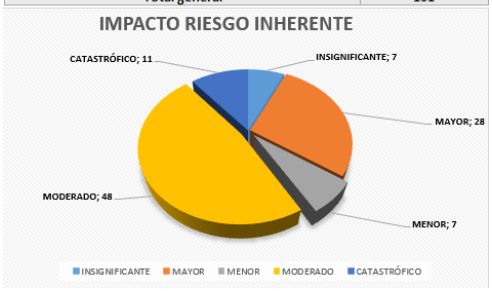
NATURALEZA DEL CONTROL RIESGOS GESTIÓN	
DESCRIPCIÓN DEL CONTROL	Total Controles
Detectivo	92
Preventivo	139
Correctivo	11
Total general	**242**

Gráfica 4 Descripción del Control vs Total Controles

5.6 Zona de impacto riesgo inherente y residual

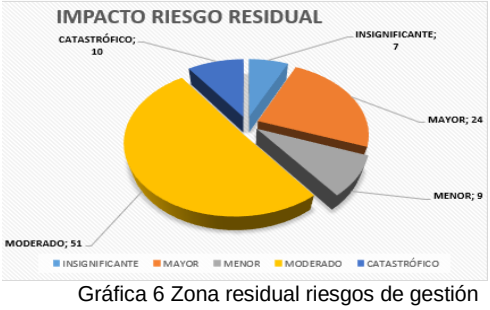
Acorde con lo establecido en la metodología utilizada por parte del Distrito de Medellín para la administración del riesgo, a los riesgos de gestión les aplica los niveles de impacto "Insignificante", "Menor", "Moderado", "Mayor" y "Catastrófico. Así mismo se establece que con la ejecución de controles 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	7
MAYOR	28
MENOR	7
MODERADO	48
CATASTRÓFICO	11
Total general	**101**



Gráfica 5 Zona inherente riesgo de gestión

IMPACTO RIESGO RESIDUAL POR ZONA	Total Riesgos
INSIGNIFICANTE	7
MAYOR	24
MENOR	9
MODERADO	51
CATASTRÓFICO	10
Total general	**101**



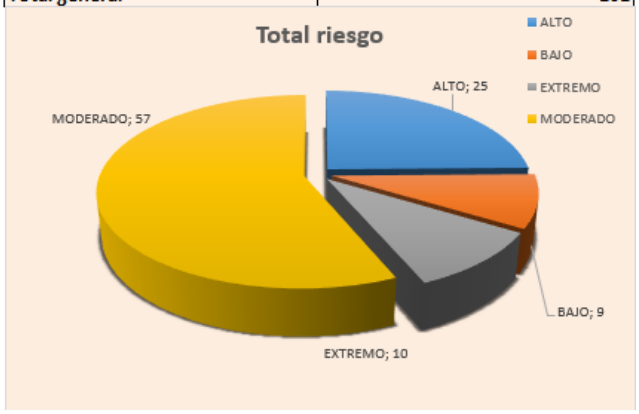
Gráfica 6 Zona residual riesgos de gestión

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 solos 3 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	25
BAJO	9
EXTREMO	10
MODERADO	57
Total general	**101**



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 (12); alto (31) y moderado (51) que equivalen al 93%, deben contar con controles que permitan REDUCIR la probabilidad de ocurrencia del riesgo.

5.8 Riesgos de gestión materializados

Para el tercer cuatrimestre de 2024, 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 julio a octubre 2024, 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.

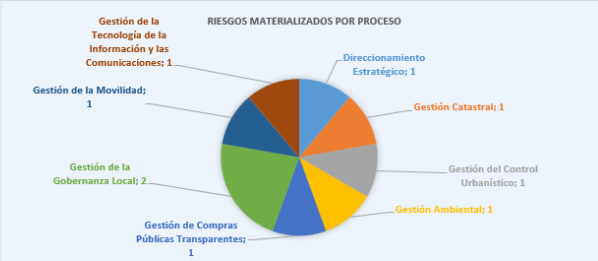
De los ciento un (101) riesgos de gestión identificados en los veintisiete (27) procesos, durante el tercer cuatrimestre se evidencia la materialización de nueve (9) riesgos, como lo muestra la gráfica 8.

RIESGOS MATERIALIZADOS	
Materializó	**Total**
No	92
Si	9
Total general	**101**

Gráfica 8 Materialización riesgos de gestión

Los *riesgos de gestión* materializados (9), se distribuyeron en ocho (8) de los veintisiete (27) procesos, tal y como se presenta en la gráfica 9; igualmente se evidencia que el proceso con mayor número de *riesgos de gestión* materializados es Gestión de la Gobernanza Local con dos riesgos, los 7 procesos restantes materializaron de a un riesgo de gestión.

RIESGOS MATERIALIZADOS	
PROCESO	Total
Direccionamiento Estratégico	1
Gestión Catastral	1
Gestión del Control Urbanístico	1
Gestión Ambiental	1
Gestión de Compras Públicas Transparentes	1
Gestión de la Gobernanza Local	2
Gestión de la Movilidad	1
Gestión de la Tecnología de la Información y las Comunicacion	1
Total general	9



Gráfica 9 Riesgos materializados por proceso

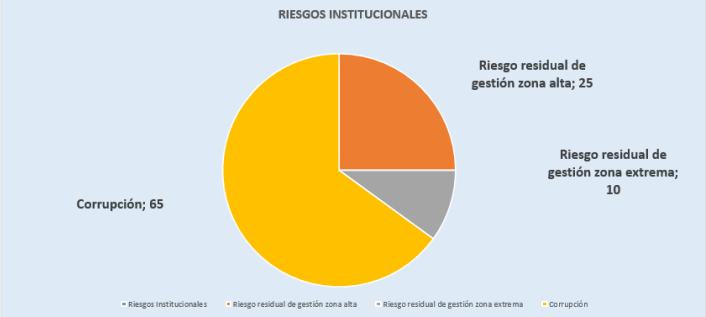
En el anexo 1 *Descripción Riesgos Materializados Por Proceso,* se encuentran los riesgos materializados, clasificados por proceso, el acta que evidencia la autoevaluación, la acción de mejora formulada por parte de los directivos que lideran procesos en conjunto con sus equipos, con el fin de mitigar 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	25
Riesgo residual de gestión zona extrema	10
Corrupción	65
Total general	100



Gráfica 10 Riesgos Institucionales

En la tabla 4 (riesgos de gestión en zona alta, 25 riesgos) y tabla 5 (riesgos de gestión en zona extrema, 10 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 Tecnología de la Información y las Comunicacion	1
Gestión del Desarrollo Económico	7
Gestión del Riesgo de Desastres	1
Gestión Social del Riesgo	1
Total general	25

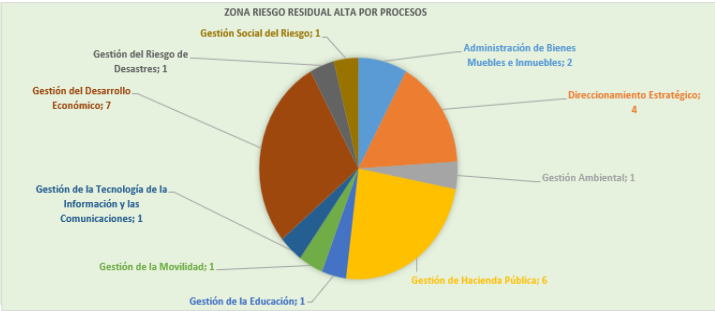


Tabla 4. Zona de riesgo residual alta

ZONA RIESGO RESIDUAL EXTREMA POR PROCESOS	
PROCESO	TOTAL RIESGOS
Administración de Bienes Muebles e Inmuebles	1
Direccionamiento Estratégico	1
Gestión de Compras Públicas Transparentes	3
Gestión de la Educación	2
Gestión de la Salud	2
Gestión de la Tecnología de la Información y las Comunicaciones	1
Total general	10

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 agosto a noviembre de la vigencia 2024.

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

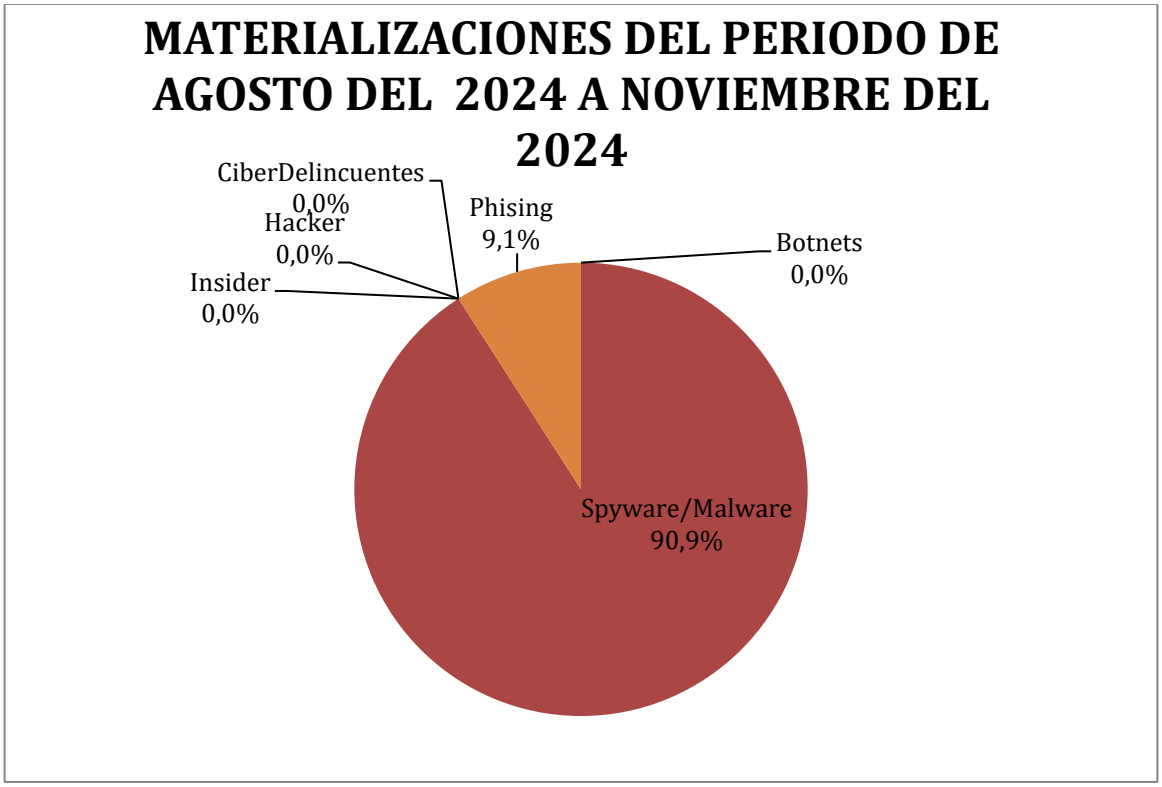
8. Seguimiento a los Riesgos de seguridad informática identificados y sus materializaciones.

En atención a los riesgos identificados y valorados, a continuación, se presentan las materializaciones en el periodo de reporte, a través de la siguiente tabla:

POSIBLE AFECTACIÓN DE LA DISPONIBILIDAD / INTEGRIDAD / CONFIDENCIALIDAD DEL ACTIVO DE TECNOLOGÍA DE INFORMACIÓN (AGOSTO 2024 – NOVIEMBRE 2024)		
No.	Activo de T.I. - Amenaza	Materializaciones
1	Servidores - Botnets	0
2	Servidores - Spyware/Malware	0
3	EndPoints - Botnets	0
4	EndPoints - Spyware/Malware	9
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	1
TOTAL DE MATERIALIZACIONES		11

Tabla 7. Afectación de la Disponibilidad

El total de materializaciones en el periodo fue de 11 en relación con los grupos de riesgos identificados, de los cuales el 90,9% están relacionados con Spyware/Malware que ha afectado equipos de usuario final y el 9,1 % está relacionado con phishing en correo Electrónico Institucional. Tal como se puede apreciar en la siguiente gráfica:

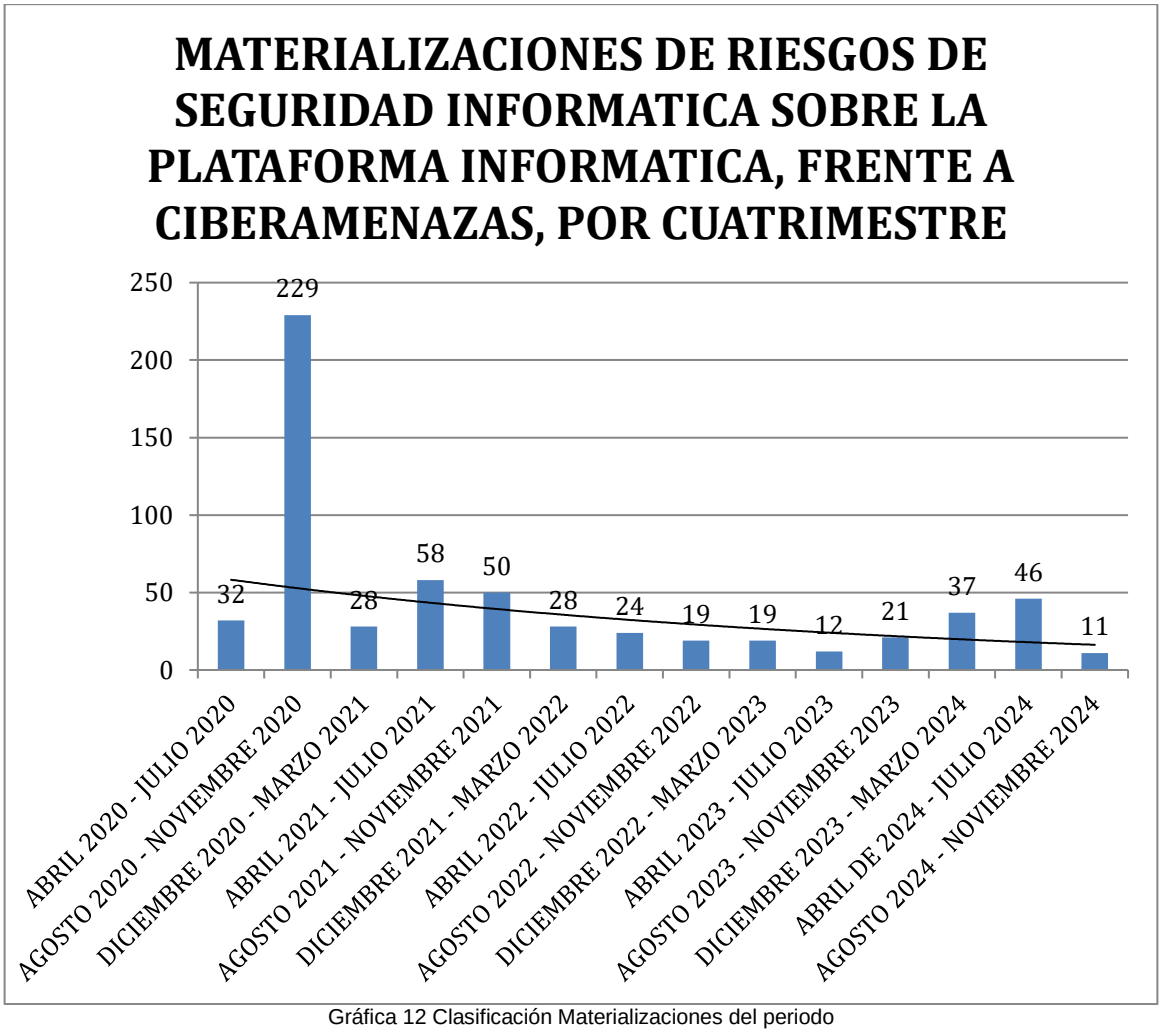


Gráfica 11 Materializaciones del periodo

ANALISIS POR FUENTE DE AMENAZAS EN EL PERIODO AGOSTO 2024 – NOVIEMBRE 2024	
Amenazas	Materializaciones
Botnets	0
Spyware/Malware	10
Hacker	0
Insider	0
CiberDelincuentes	0
Phishing	1
TOTAL	11

Tabla 8. Análisis por fuente de amenazas en el periodo

Se puede observar referente a las materializaciones que se evidencia una disminución del 76% en comparación con las materializaciones del cuatrimestre anterior, tal como se presenta en la siguiente gráfica:



Gráfica 12 Clasificación Materializaciones del periodo

Esto indica los cambios en el entorno de amenazas al que se enfrenta la organización, ya que las materializaciones están conectados a dichos cambios, produciendo variaciones en los ataques que se reciben sobre los diferentes activos de tecnologías de información expuestos por la organización. Ante las materializaciones de malware en equipos de cómputo y servidores, es crucial implementar medidas proactivas para proteger la infraestructura y los datos de la entidad.

Gráfica 13 Materializaciones en el periodo

En la gráfica anterior, se pueden apreciar las materializaciones detalladas por activos de información y amenazas, siendo la materialización de amenazas de malware sobre estaciones de usuario final la causante del 81.8% de las materializaciones y 9,1% a través del uso de medios removibles en estaciones de usuario final. Adicionalmente se evidencio la materialización de phishing en correo electrónico de 9,1 % del total de las materializaciones en el cuatrimestre consolidado:

Lo anterior es importante resaltarlo, teniendo en cuenta que dichas materializaciones sobre estaciones de usuario final están relacionadas con la corresponsabilidad en el uso

de los recursos informáticos por parte de los servidores públicos y contratistas a quienes les han sido asignados para la prestación de sus servicios laborales.

Por otro lado, es importante resaltar que la materialización del riesgo frente a la recepción de notificaciones clasificadas como phishing dirigidas hacia cuentas de correo electrónico de usuario organizacionales se ha visto disminuido en 94,7 % este cuatrimestre con respecto al anterior. Es importante destacar, que en el cuatrimestre actual, el control implementado por la organización para la protección del servicio de correo electrónico bloqueo cerca de 729.415 correos electrónicos recibidos desde usuarios externos hacia la entidad que representan el 26,4% del total de correo electrónicos recibidos en el cuatrimestre, que fue de 2.761.956 correos electrónicos recibidos; por lo cual es importante, volver a resaltar el valor de la corresponsabilidad de los usuarios finales como actores fundamentales frente al uso adecuado de los servicios de Tecnologías de Información dispuestos por la entidad.

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 tercer cuatrimestre de 2024, 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 y dos (242) 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 un (101) riesgos de gestión identificados en los veintisiete (27) procesos, se evidencia la materialización de 9 riesgos, correspondiente al 9% del universo de riesgos de gestión de la entidad.

- Al comparar el número de riesgos de gestión identificados en los veintisiete procesos del Modelo de Operación del Distrito de Medellín autoevaluados en el tercer cuatrimestre de 2024 con la autoevaluación del segundo cuatrimestre del 2024, se evidencia que no hubo una variación.

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					
TERCER CUATRIMESTRE 2024 Trece (9) riesgos materializados					
N°	**Proceso**	**Acta Isolución**	**Riesgo materializado**	**Acción para abordar riesgos**	**Observación**
1	Direccionamiento Estratégico	Dep-DIES - 53	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 "Conceptos técnicos de acuerdo al POT" en la Unidad de Atención y Aplicación de la Norma Urbanística de la Subdirección de Planeación Territorial y Estratégica de Ciudad del DAP. Las causas de materialización del riesgo que se identificaron son: *Sobre carga laboral e insuficiente recurso humano para responder a la demanda de solicitudes que ingresaron en el periodo autoevaluado. *Fallas en el visor Mapgis, en el sistema de gestión documental Mercurio y la intermitencia en la conectividad a internet. *Dificultad en el acceso al material de consulta o información requerida para dar respuesta.
2	Gestión Catastral	Sub-GCAT - 32	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	2722	Se estableció mesa de trabajo el día 06 de septiembre con la Secretaría de Hacienda y las diferentes dependencias, mediante la cual se socializó el presupuesto requerido para la ejecución de los diferentes proyectos en la vigencia 2025 para la Subsecretaría de Catastro, en ella acordaron proporcionar recursos adicionales a los techos presupuestales establecidos inicialmente en el POAI y el Plan Plurianual 2024-2027. Se presentó incumplimiento en la oportunidad de respuesta del 53,10% de los 3,780 trámites ingresados en el periodo de 01 de agosto de 2024 al 30 de noviembre de 2024, se tienen 14,782 solicitudes pendientes correspondientes al corte del 01 de diciembre de 2024. El tiempo promedio de respuesta de las solicitudes durante el periodo a analizar fue de 185,87 días. Se estableció un plan de descongestión, a fin de agilizar la gestión de los trámites catastrales, dando respuesta a 2.212 solicitudes represadas de años 2019, 2020 y 2021, que reposan en las bases de datos de la Subsecretaría de Catastro, el cumplimiento de este plan de descongestión ha sido efectivo, ya que a la fecha se encuentra en un 78%.

					Para el año 2025 se pretende realizar la descongestión de todos los trámites represados correspondientes a los años 2022, 2023 y 2024 que reposan en las bases de datos de la Subsecretaría de Catastro y atender los trámites que ingresan en el año 2025, esto con el fin de poner al día en la Subsecretaría y así tener un flujo de trámites acorde a la dinámica inmobiliaria, dando oportuna respuesta y garantizando la calidad e la respuesta de los trámites
3	Gestión del Control Urbanístico	Sub-GCUR-13	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 (pandemia, desastres naturales, otros eventos de impacto nacional y mundial)	2749	Aunque se ha mejorado los controles para el seguimiento de las PQRSD, en la Subsecretaria el volumen que ingresa de solicitudes como oficios, PQRSD, solicitudes por órganos de control, es alto y por la falta de personal que se ha venido presentando por demoras en el proceso de Contratación, que como consecuencia el riesgo se sigue materializando. Los controles si han minimizado los tiempos de respuestas con respecto al periodo anterior, se continuará con la aplicación de los controles. Se genera Acción para abordar riesgos #2749 en Isolución para dar cobertura a la materialización de este riesgo. Según el 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: Total PQRSD Agosto - Noviembre 2024 = 935 =100% Total PQRSD gestionadas oportunamente= 795 = 85.03% Total PQRSD gestionadas inoportunamente = 140 = 14.97% Este detalle comprende el periodo entre Agosto y Noviembre del 2024 toda vez que Según el Decreto 491 de 2020, establece en su artículo 5 “Ampliación de términos para atender las peticiones”.
4	Gestión Ambiental	SEC-GEAM017	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	2750	Debido a que no se elaboraron los estudios de zonificación acústica y objetivos de calidad acústica para el Distrito a causa de la “baja disponibilidad de recursos financieros” e “insuficiente disponibilidad de personal idóneo”. Si bien es cierto, al ejecutar los controles establecidos en el mapa, se logró que el AMVA incluyera en los alcances de un contrato interno la realización del diagnóstico para la zonificación acústica, esto permitió avanzar sólo en un 10%, cuando lo esperado era llegar al 40%.

			Unidades y Equipos de Trabajo al interior de la Secretaría de Medio Ambiente.		
5	Gestión de Compras Públicas Transparentes	Sec-GEC-31	Posibilidad de afectación económica y reputacional por incumplimiento en la aplicación de las políticas de operación, directrices, planes y la normativa legal del proceso de Gestión de Compras Públicas Transparentes a que está obligado debido a falta de unidad de criterios en la aplicación de las políticas o procedimientos , designación de los gestores y supervisores sin las competencias establecidas en el Manual de Contratación y el documento específico Generalidades Supervisión e Interventoría , sobrecarga laboral , decisiones inadecuadas en la aplicación de las políticas de operación y directrices del proceso de Gestión de Compras Públicas Transparentes a que está obligado, evento exógeno sobreviniente	2736	La materialización de este riesgo se dio porque en el periodo comprendido entre el 15 de julio de 2024 y el 15 noviembre de 2024, en la Secretaría Privada se publicaron extemporáneamente los informes de supervisión de los contratos4600101180 en los meses julio y septiembre y 4600101588 para el mes de septiembre, incumpliendo los tres días establecidos en la ley 1150 de 2007 y decreto reglamentario 1510 de 2013. Esta situación puede generar hallazgos por parte de los organismos de control Causa: sobrecarga laboral, algunos supervisores tuvieron múltiples ocupaciones que dificultaron el cargue de los informes de supervisión, dentro del término establecido por la ley.
6	Gestión de la Gobernanza Local	Sec-GGOL43	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 de tipo biológico o ambiental, sobrevinientes	5254	Según el Informe de PQRSD que comprende el período junio a noviembre de 2024, el Proceso GGOL NO superó la meta de oportunidad del 92%. Su porcentaje de oportunidad de respuesta a las PQRSD fue de 90,25%.
7	Gestión de la Gobernanza Local	Sec-GGOL43	Posibilidad de afectación reputacional por inoportunidad en el desarrollo de los procesos asociados a las indisciplinas sociales, las problemáticas familiares, o el uso inadecuado del espacio público, debido a alto volumen de procesos y trámites vs	5255 y 5256,	Según la última medición de indicadores del proceso GGOL, algunos no cumplieron la meta por lo que se continúa con las acciones de mejora para superar la situación

			debilidad en la capacidad de respuesta, alto volumen de procesos y trámites vs incidencia de factores exógenos de tipo biológico o ambiental, sobrevinientes, que afectan la atención.		
8	Gestión de la Movilidad	Unidad Administrativ-GMOV10	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	El riesgo continúa materializándose, aun así no hay cifras exactas para estos tres meses, dado que para los meses octubre y noviembre no hay indicador calculado, puesto que Mercurio 8,0 presenta contingencia y no hay manera de hacer reportes aún. Sin embargo, para el mes de septiembre de 2024 el indicador estaba por encima del 92% (exactamente 99,29%) y al calcular el porcentaje acumulado hasta 30 de septiembre el indicador da como resultado 79,29%.
9	Gestión de la Tecnología de la Información y las Comunicaciones	SID-GTIC15	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 normatividad sobre Infraestructura Física en los Archivos.	2733	Se presentó indisponibilidad de la información producida y recibida en la entidad debido a: - La migración de la herramienta de gestión MERCURIO de la versión 6.5 a la versión 8.0